Politiets hemmelige efterforskning på internettet

Lentz, Lene Wacher

Publication date:
2019

Document Version
Også kaldet Forlagets PDF

POLITIETS HEMMELIGE EFTERFORSKNING PÅ INTERNETTET

AF
LENE WACHER LENTZ

PH.D. AFHANDLING 2019

AALBORG UNIVERSITET

Politiets hemmelige efterforskning på internettet

Artikelbaseret ph.d.-afhandling

Af Lene Wacher Lentz, Juridisk Institut, Aalborg Universitet

Ph.d. indleveret: Juli 2019

Ph.d. vejleder: Professor Birgit Feldtmann
Aalborg Universitet

Ph.d. bedømmelsesudvalg: Lektor Thomas Neumann
Aalborg Universitet

Professor Thomas Elholm
Københavns Universitet

Professor Inger Marie Sunde
Politihøgskolen i Oslo

Ph.d. serie: Det Samfundsvidenskabelige Fakultet,
Aalborg Universitet

ISSN (online): 2246-1256
ISBN (online): 978-87-7210-556-7

Udgivet af:
Aalborg Universitetsforlag
Langagervej 2
9220 Aalborg Ø
Tlf. 9940 7140
aauf@forlag.aau.dk
forlag.aau.dk

Trykt i Danmark af Rosendahls, 2019

Resumé

Internettet har givet næring til ny kriminalitet, såsom 'hacking' af datasystemer, databedrageri, afpresning, samt deling af krænkende billedmateriale mv. Derudover giver internettets mange kommunikationsplatforme mulighed for at kommunikere med medgerningsmænd, komme i kontakt med mulige ofre mv. Denne nye digitale 'scene' for kriminalitet og kommunikation om kriminalitet, giver politiet store udfordringer, og en række nye metoder udvikles for at udnytte den nye digitale kontekst til efterforskning og opklaring.

Retsplejeloven, som regulerer politiets efterforskning og tvangsindgreb, indeholder ingen særlige bestemmelser om internettet. I stedet anvendes de eksisterende regelsæt i den nye digitale kontekst, hvilket aktualiserer en række retlige problematikker.

Formålet med denne artikel-baserede afhandling er at analysere den retlige regulering af politiets hemmelige efterforskning på internettet. To typetilfælde af hemmelig efterforskning er udvalgt: Først det 'tekniske tvangsindgreb', hvor politiet skaffer sig hemmelig teknisk adgang til private datasystemer på internettet, hvilket i retsplejeloven er reguleret af tre regelsæt, hemmelig ransagning, indgreb i meddelelseshemmeligheden og dataaflæsning. Dernæst det 'menneskelige indgreb', hvor politiet under dække interagerer med borgeren for at skaffe beviser mv., hvilket er omfattet af de tre efterforskningsmetoder, infiltration, lokkedue-situationen og agentvirksomhed. Et gennemgående tema i afhandlingen er, hvornår nye efterforskningsmetoder kræver lovhjemmel. Med udgangspunkt i Hans Gammeltoft-Hansens definition af et tvangsindgreb, genovervejes dette straffeprocessuelle legalitetsprincip i et digitalt og menneskeretligt perspektiv.

Afhandlingen er bygget op om seks artikler: **Artikel 1**: "'Hacking' og det digitale privatliv", angår, hvornår man efter straffelovens 'hacking'-bestemmelse har skaffet sig uberettiget adgang til andres datasystemer. **Artikel 2**: "Logning af teledata i lyset af Tele2-dommen", og **Artikel 3**: "Retsplejelovens regulering af politiets adgang til teledata", angår politiets indgreb i meddelelseshemmeligheden, hvor det af de to artikler fremgår, at EU-Domstolen i Tele2-sagen har udtalt, at logning af teledata og politiets adgang hertil kun må ske ved "alvorlig kriminalitet", hvorfor retsplejelovens regulering må forventes ændret i overensstemmelse hermed. **Artikel 4:** "Politiets hjemmel til 'hacking' som led i en efterforskning", indeholder en analyse af de tre regelsæt, hemmelig ransagning, indgreb i meddelelseshemmeligheden som hjemmel til politiets 'hacking'. **Artikel 5**: "Politiets infiltration på digitale platforme – set i et menneskeretligt perspektiv", angår den ulovregulerede efterforskningsmetode, infiltration, hvor metoden illustreres i et digitalt scenarie. **Artikel 6**: "Politiagenter i et menneskeretligt perspektiv", omhandler retsplejelovens regulering af politiets agentvirksomhed, hvor fokus er på den processuelle ramme for iværksættelse af

agentvirksomheden og hvordan det sikres, at aktionen begrænses til det nødvendige til efterforskningen.

Afhandlingens konklusion er, at der er behov for at genoverveje reguleringen af de 'tekniske tvangsindgreb', og der argumenteres for, at der etableres en udtrykkelig hjemmel til politiets 'hacking'. I forhold til de 'menneskelige indgreb' er afhandlingens konklusion, at infiltration i lyset af Den Europæiske Menneskerettighedskonventions artikel 8 må nærmere reguleres. Endvidere argumenteres for at styrke den processuelle ramme om politiets agentvirksomhed, bl.a. ved et konkret tiltag om advokatbeskikkelse. Overordnet set konkluderer afhandlingen, at spørgsmålet om hvilke efterforskningsmetoder, der skal reguleres i retsplejelovens, ikke længere blot kan besvares ud fra Gammeltoft-Hansens definition af et tvangsindgreb. Navnlig i lyset af den digitale udvikling samt retsudviklingen i tilknytning til Den Europæiske Menneskerettighedskonvention må flere efterforskningsmetoder reguleres.

Abstract

The internet has fuelled new crimes such as attack on data systems, computer fraud and 'ransomware', besides sharing of sexual abusive material etc. Furthermore, the many communication platforms of the internet enable the possibilities of communicating with co-perpetrators, getting in contact with possible victims, etc. The new digital scene for crime and the communication hereof leaves the police with great challenges, and, currently, the police is developing a number of new methods for the online platforms that will enable them to utilise the new digital context for investigation and detection of crimes.

The Danish Code of Criminal Procedure, which regulates the police's investigation and coercive methods, does not contain specific clauses regarding the internet. Instead, the law is developed by applying the current legal framework to the new digital context. However, this results in a number of legal problems.

The purpose of this article-based dissertation is to analyse the legal regulation of the police's secret investigation on the internet. Two cases of secret investigation have been chosen for this dissertation. The first case is the 'technical coercive method', which entails that the police gain secret technical access to private data systems, platforms, etc. on the internet, which in the Danish Code of Criminal Procedure is regulated by three sets of rules; (1) covert search, (2) interception of communication and (3) computer surveillance. The second case is the 'human intervention', which entails that the police whilst undercover interacts with the citizen in order to obtain evidence, etc., which is comprised of three methods of investigation, (1) infiltration, (2) decoy situations and (3) undercover agents. A recurring theme in the dissertation is when does new methods of investigation require legal regulations. Based on Hans Gammeltoft-Hansen's definition of a coercive method, this principle of legality of criminal procedure is reconsidered in a digital and human rights perspective.

The dissertation contains 6 articles; **Article 1:** "Hacking and the Digital Privacy" regards how one in accordance with the hacking provision of the Danish Criminal Code has gained unauthorised access to data systems. **Article 2:** "Data Retention Related to Electronic Communication in the Light of the Judgment in the Tele2 case", and **Article 3:** "The regulation of the Danish Code of Criminal Procedure of the Police's access to Traffic Data Related to Electronic Communication" regard the police's interception of communication. Both Articles express that the European Court of Justice in the Tele2 proceedings has stated that data retention related to electronic communication and the police's access hereto must only occur in the event of serious crime, therefore, it must be expected that the Danish Code of Criminal Procedure is regulated accordingly. **Article 4:** "The Police's Legal Basis for Hacking as Part of an Investigation" contains an analysis of the three sets of rules; (1) covert search, (2) interception of communication and (3) computer surveillance as legal basis for

the police's hacking, in which the problematic interaction between the three regulations is emphasised. **Article 5:** "Police-infiltration on Digital Platforms – in a Human Rights Perspective" regards infiltration, which has not yet been subject to regulation, and the method is illustrated in a digital scenario. **Article 6:** "Agents Provocateurs in a Human Rights Perspective" regards the regulation of the Danish Code of Criminal Procedure of the undercover agents of the police, in which the focal points are the procedural framework for the implementation of undercover agents and how it is assured that actions are limited to the necessaries of the investigation.

The conclusion of the dissertation is that it is necessary to reassess the regulation of the 'technical coercive methods', and it can be argued that a definite legal basis for the police's hacking must be established. In regard to the 'human interventions', the dissertation concludes that infiltration in the light of Article 8 of the European Convention of Human Rights must be subjected to regulation. Furthermore, arguments of strengthening the procedural framework of the undercover agents of the police are presented – e.g. appointment of legal representatives by court as a concrete initiative. Overall, the dissertation concludes that in the light of the digital development as well as the development of the law in connection with the European Convention of Human Rights, it must be expected that several investigation methods must undergo express regulations.

Indholdsfortegnelse

Del 1 – Indledning **13**

Kapitel 1 IT-Kriminalitet og straffeprocessens perspektiv **15**
1. Den nye digitale kriminalitet *15*
2. Straffeprocessens perspektiv og bærende hensyn *16*
2.1. Beskyttelsen af privatliv 16
2.2. Politiets kriminalitetsbekæmpelse 18
2.3. Retsplejelovens regulering 20
3. Det straffeprocessuelle legalitetsprincip *22*

Kapitel 2 Afhandlingens formål **23**
1. Problemformulering og centrale temaer *23*
2. Forskningsspørgsmål *25*
3. Afhandlingens struktur *26*
3.1. Politiets "tekniske tvangsindgreb" 26
3.1.1. 'Hacking'-bestemmelsen i straffelovens § 263 26
3.1.2. Hjemmel for politiets 'hacking' 27
3.1.3. Kort om teledata 29
3.2. Politiets 'menneskelige indgreb' på internettet 30
3.3. Det straffeprocessuelle legalitetsprincip 31
4. Afgrænsning *31*
4.1. Internationale aspekter 32

Kapitel 3 Metodiske overvejelser **35**
1. Metode *35*
1.1. Retsdogmatisk metode 35
1.2. Internettet og retlig pluralisme 35
1.3. Retspolitiske betragtninger og friere overvejelser 39
1.4. Komparativ metode 39
2. Retskilder og fortolkningsprincipper *40*
2.1. Danske retskilder 40
2.1.1. Danske fortolkningsprincipper 42
2.1.2. Litteratur – "State of the art" 42
2.2. EU-rettens betydning for dansk strafferet og straffeproces 43
2.2.1. EU-retskilder 46
2.2.2. EU-fortolkningsprincipper 49
2.3. Europarådets Cybercrimekonvention 50

2.4. Den Europæiske Menneskerettigheds Konvention (EMRK) 51
2.4.1. Den Europæiske Menneskerettighedsdomstols fortolkningsprincipper 53
2.4.2. Danske fortolkningsprincipper i forhold til EMRK 55
2.5. Øvrige retskilder 56
3. Afhandlingens form og forløb 56
3.1. Begrundelse for artikelbaseret 56
3.2. Opdateret viden om det politioperative aspekt 57
4. Forfatterens forskningsmæssige integritet 58

Del 2 – Artiklerne 61
Oversigt over Artikel 1-6 *..... 63*
Artikel 1*: 'Hacking' og det digitale privatliv 67*
Artikel 2*: Logning af teledata i lyset af Tele2-dommen 81*
Artikel 3*: Retsplejelovens regulering af politiets adgang til teledata 91*
Artikel 4*: Politiets hjemmel til 'hacking' som led i en efterforskning 101*
Artikel 5*: Politiets infiltration på digitale platforme – set i et menneskeretligt perspektiv 109*
Artikel 6*: Politiagenter i et menneskeretligt perspektiv 137*

Del 3 – Besvarelse af forskningsspørgsmål 165

Kapitel 1 Den overordnede retlige ramme for politiets hemmelige efterforskning på internettet 167
1. Retsplejeloven 167
2. Det straffeprocessuelle legalitetsprincip 167
2.1. Kort om analogi og det strafferetlige legalitetsprincip, jf. straffelovens § 1 171
2.2. Retsplejelovens 'udtømmende katalog' 174
2.3. Fortolkning i lyset af den teknologiske udvikling 174
2.3.1. Adgang til digitale brugerprofiler med rette kode 175
2.3.2. Udvidet teleoplysning og teleobservation 175
2.3.3. Dataaflæsning 176
2.3.4. Åbning af mobiltelefon med fingeraftryk 177
2.3.5. Gps-overvågning 178
2.4. Sammenfatning af den hidtidige retspraksis 180
2.5. De bagvedliggende hensyn i strafferetten og straffeprocessen 181
3. Det menneskeretlige perspektiv 183
4. Sammenfatning vedrørende det straffeprocessuelle legalitetsprincip 186
5. Praktiske aspekter ved politiets ibrugtagning af nye, digitale efterforskningsmetoder 187

Kapitel 2 Straffelovens bestemmelse om 'hacking' som pejlemærke for politiets efterforskning 191
1. Relevans for politiets efterforskning 191
2. Sammenfattende og opfølgende om straffelovens 'hacking'-bestemmelse 192
3. Den strafferetlige legalitetsprincip, jf. straffelovens § 1 194
3.1. Dansk retspraksis om analogi som følge af ny teknologi 196
3.2. Legalitetskrav og forudsigelighed, jf. EMRK artikel 7, stk. 1 198
4. 'Hacking'-bestemmelsen i lyset af legalitetsprincippet 205
5. Retspolitiske betragtninger 206
6. Betydning for politiets 'hacking' 209

Kapitel 3 Reguleringen af politiets tekniske indgreb på internettet 211
1. Sammenfattende om retsplejelovens tekniske indgreb 211
2. EMRK artikel 8, stk. 2 212
2.1. Den tekniske adgang i forhold til EMRK artikel 8, stk. 2 214
3. Er der noget teknisk indgreb, der ikke dækkes af retsplejelovens regulering? 215
3.1. Digital observation 216
3.2. Politiets brud på kryptering mv. 219
4. Retspolitiske overvejelser om nytten af en egentlig hjemmel til 'hacking' 224
4.1. Tekniske aspekter ved politiets 'hacking' 225
5. Sammenfatning vedrørende politiets tekniske indgreb 227

Kapitel 4 Reguleringen af politiets 'menneskelige indgreb' på internettet 229
1. Sammenfattende om politiets 'menneskelige indgreb' 229
2. Lokkedue-situationen 229
3. Infiltration i et forvaltningsretligt perspektiv 232
3.1. Skattemedarbejder på Facebook, FOB 2011.1501 232
3.2. Offentlige myndigheders undersøgelser på kommercielle platforme 234
4. Agentvirksomhed i et digitalt perspektiv 235
4.1. Digitale udfordringer og retlig regulering 235
4.2. Internationalt samarbejde 236
5. Opfølgning på begrebet det 'menneskelige indgreb' 238
6. Sammenfatning vedrørende politiets 'menneskelige indgreb' på internettet 239

Del 4 – Afslutning 241

Kapitel 1 Sammenfatning og perspektivering 243
1. Sammenfatning af de retspolitiske overvejelser 243
2. Digitale udfordringer 244
3. Teknologineutralitet som aspekt ved fremtidige reguleringer 245
4. Dansk straffeproces og internationale strømninger 249
5. Bevisvurdering og den materielle sandheds princip 250
6. Tillid til politi og straffesystem 252

Bilag 255
1. Brev til Facebook 255
2. Uddrag af Den Danske Værdiundersøgelse 256
3. Domsliste 257
4. Litteraturliste 264

Del 1 – Indledning

Kapitel 1 IT-Kriminalitet og straffeprocessens perspektiv

1. Den nye digitale kriminalitet

Internettet har givet grobund for nye kriminalitetsformer, hvor her især kan nævnes misbrug af betalingskort (databedrageri), 'hacking' af datasystemer, hvor der kræves løsesum for at frigive data og systemer ("ransomware"), udbredelse af billedmateriale med seksuelle krænkelser mod børn, samt deling af privat billedmateriale uden samtykke.[1] Derudover er de sociale medier og internettets mange chatfora nu blevet centrale steder, hvor gerningsmanden kommer i kontakt med forurettede, hvor flere gerningsmænd aftaler, hvordan forbrydelsen skal foregå og forberedes, og efterfølgende hvordan forklaringer til politiet skal samstemmes, spor slettes, vidner udsættes for trusler mv.

Både ved efterforskningen af den egentlige IT-kriminalitet og ved efterforskningen af denne sociale kontekst, hvor der kommunikeres om forbrydelsen, er der derfor vigtige spor og beviser at finde for politiet.

Når forbrydelsen og kommunikationen om forbrydelsen sker på internettet, har gerningsmanden den fordel at kunne sløre sin identitet. Oftest vil han skulle oprette en brugerprofil for at agere på de forskellige platforme, men her vil det i vidt omfang være muligt at bruge falsk navn og adresse. Han kan bruge telefonnummer fra et uregistreret taletidskort. Derudover kan han oprette en email-adresse fra en af de mange hjemmesidebaserede email-tjenester (såsom yahoo, hotmail, gmail.com etc.), hvor brugerens identitet ikke verificeres. Endelig kan han sætte sig på det lokale bibliotek, hvor internetadgangen på computeren deles med adskillige andre brugere, eller han kan bruge en af de mange internettjenester, hvor man agerer via udenlandske servere, og hvor brugerens identitet og danske tilhørsforhold vil blive sløret.

Netop muligheden for at sløre sin identitet på internettet, er en stor udfordring for politiets efterforskning, hvilket er baggrunden for, at der i disse år udvikles og afprøves nye digitale efterforskningsmetoder.

[1] Afsnit 1 er et lettere omarbejdet uddrag af "Efterforskningens grænser på internettet", af Lene Wacher Lentz, s. 140-141, bidrag til antologien "*Eksponeret – Grænser for privatliv i en digital tid*", af Rikke Frank Jørgensen og Birgitte Kofod Olsen (red.), 2018.

Den digitale efterforskning giver en lang række nye problematikker at forholde sig til: Hvordan skal retsplejelovens regler for politiets efterforskning i den fysiske verden overføres på den efterforskning, der sker på internettet? Giver det i det hele taget mening at overføre regler fra den fysiske verden til den digitale verden, eller må man frigøre sig fra dette tankesæt og lave en lovgivning, der passer præcist til internettet, og som udtrykkeligt afbalancerer hensynet til borgeren over for hensynet til strafforfølgningen? Hvornår er man på internettet på offentligt område, og hvornår er man på privat område? Hvordan skal den virtuelle politimand agere, navnlig i forhold til at være synligt og virtuelt 'uniformeret' politi på internettet, og hvornår det vil være i orden for politiet at agere under dække af at være almindelig bruger?

Talrige er de nye, digitale problematikker, der præger straffeprocessen i disse år. I det følgende afsnit udfoldes straffeprocessens perspektiv og bærende hensyn, og med dette afsæt redegøres i kapitel 2 for denne artikelbaserede afhandlings formål, forskningsspørgsmål og struktur.

2. Straffeprocessens perspektiv og bærende hensyn

Grundlæggende har straffeprocessen til formål at regulere efterforskning og strafforfølgning af forbrydelser, hvor det samtidig sikres, at den enkelte borger ikke lider unødig overlast. Straffeprocessen er detaljeret reguleret i retsplejeloven, der overordnet set er udtryk for en afvejning mellem de to hensyn: borgerens privatliv over for politiets kriminalitetsbekæmpelse. Disse to hensyn afdækkes indledningsvist i det følgende, hvorefter afsnit 2.3. introducerer retsplejeloven som den retlige ramme for reguleringen af politiets efterforskning.

2.1. Beskyttelsen af privatliv

Privatliv som et gode og en nødvendighed i et demokratisk samfund, hersker der næppe uenighed om.[2] Som formuleret af Sten Schaumburg-Müller om begrebet borgerlig privathed, refererer dette til *"den idé, at en velfungerende borgerlig offentlighed forudsætter en privathed, et delvis uigennemsigtigt område, hvor man er afskærmet fra offentligheden og i ro mag bl.a. kan tænke langsomt uden offentlighedens til tider alt for hurtige, intuitive reaktioner*."[3]

[2] Om privatlivet og 'privathed' som et gode, se bl.a. Peter Blume: "Overvågning. Kan persondataretten gøre nytte?", Nordisk Tidsskrift for Informationsvidenskab og Kulturformidling, årg. 3, nr. 2/3, 2014, Peter Blume og Janne Rothmar Herrmann: *"Ret, privatliv og teknologi"*, 2018, s. 13 ff. og 64 ff., Sten Schaumburg-Müller: "Borgerlig privathed i en digitaliseret verden", Nordisk Juridisk Tidsskrift Retfærd, nr. 1, 2016.

[3] Sten Schaumburg-Müller: "Borgerlig privathed i en digitaliseret verden", Nordisk Juridisk Tidsskrift Retfærd, nr. 1, 2016, s. 35.

Den retlige beskyttelse af privatlivets fred i en dansk kontekst følger overordnet set af Grundlovens frihedsrettigheder, Den Europæiske Menneskerettighedskonvention samt EU-Chartret om grundlæggende rettigheder. Ud fra denne overordnede retlige ramme for beskyttelse af privatlivet, følger beskyttelsen af en række forskellige retlige reguleringer, hvoraf de mest centrale fremhæves i det følgende.

Straffelovens bestemmelser skal i det hele ses som statens grænse for, hvad borgerne kan udsætte hinanden for, hvor særligt straffelovens kapitel 27 om freds- og æreskrænkelser kan ses som en beskyttelse af privatlivet. Straffelovens § 275 understreger, at den forurettede ved disse kriminalitetsformer i vidt omfang har medbestemmelse qua privat påtale og betinget offentlig påtale over, om forbrydelsen strafforfølges.

I forhold til myndighedernes indgreb i borgerens privatliv, følger det af forvaltningsretten og retssikkerhedsloven,[4] at indgreb skal have lovhjemmel, ligesom der stilles krav om saglighed og proportionalitet ved indgrebet. Dertil kommer databeskyttelsesreguleringen, som angår, hvornår personoplysninger må registreres og behandles, hvilket ud over myndighederne også gælder for erhvervsdrivende og i et vist omfang for private.

Med hensyn til politiets indgreb i privatlivet regulerer retsplejeloven, politiloven og retshåndhævelsesloven,[5] i hvilke tilfælde og hvordan politiet må frihedsberøve, ransage, registrere borgerens oplysninger mv.

I takt med at en større andel af vores gøremål og sociale liv henlægges til det digitale område, sker en udvikling af privatlivet, således at man ud over det traditionelle privatliv også kan tale om et digitalt privatliv, når man f.eks. bruger sin netbank, sin email eller sociale profil til kommunikation. Ret beset er det digitale fællesskab og kontakten med andre og med myndighederne ikke længere noget, vi aktivt skal melde os ind i, men noget der følger automatisk med vores almindelige daglige liv, og som vi derfor kun vanskeligt kan melde os ud af. Kravet om digital postkasse til brug for kommunikation med det offentlige, samt obligatoriske online ansøgningsprocedurer til offentlige stillinger og ydelser, medfører, at alle skal kunne tilgå digitale platforme af forskellig karakter.

[4] Lov nr. 442 af 9. juni 2004 om retssikkerhed ved forvaltningens anvendelse af tvangsindgreb og oplysningspligter.

[5] Lov nr. 410 af 27. april 2017 om Retshåndhævende myndigheders behandling af personoplysninger, som er en gennemførelse af Europa-Parlamentets og Rådets direktiv (EU) 2016/680 af 27. april 2016.

Det er imidlertid vanskeligt at definere, hvor grænserne for det digitale privatliv præcist går, og brugernes oplevelse af privathed, f.eks. ved at kommunikere på et chatforum, flugter ikke altid med virkeligheden, hvor både opsætningen af siden og de omfattende brugervilkår afslører en høj grad af offentlighed og eksponering, foruden lagring og videregivelse af data.[6] Denne vanskelighed med at vurdere, om noget er offentligt eller privat område på internettet er et af denne afhandlings centrale temaer, jf. nedenfor Kapitel 2.

Beskyttelsen af det digitale privatliv følger umiddelbart af de samme reguleringer, som beskytter det traditionelle privatliv, således finder straffeloven også anvendelse på fredskrænkelser på internettet, og ligeså vel forvaltningsretten og retssikkerhedsloven for de offentlige myndigheder, retsplejeloven og retshåndhævelsesloven for politiets efterforskning. Dog er en sådan regulering, der i sit udgangspunkt er uafhængig af, om det er fysiske eller digitale realiteter, der omfattes, ikke altid hensigtsmæssig, hvilket er en del af motivationen bag denne afhandling.

2.2. Politiets kriminalitetsbekæmpelse

Det følger af retsplejelovens § 742, stk. 2, at politiet efter anmeldelse eller af egen drift iværksætter efterforskning, når der er rimelig formodning om, at et strafbart forhold, som forfølges af det offentlige, er begået. Videre følger det af § 743, at efterforskningen har til formål at klarlægge, om betingelserne for at pålægge strafansvar eller anden strafferetlig retsfølge er til stede, og at tilvejebringe oplysninger til brug for sagens afgørelse samt forberede sagens behandling ved retten.

Politiets efterforskning beror operativt set på indhentelse af oplysninger, der vil kunne anvendes som bevis, det være sig tekniske data, spor, vidneforklaringer, ekspertudtalelser mv. De mest indgribende efterforskningsmetoder, eksempelvis ransagning, telefonaflytning mv., er reguleret i retsplejeloven som "straffeprocessuelle tvangsindgreb", jf. om retsplejeloven nedenfor.

Den traditionelle efterforskning sker med udgangspunkt i den strafbare gerning, og hvad der er brug for, for at opklare og strafforfølge forbrydelsen, jf. retsplejelovens § 743. I nogle situationer kan mere proaktive efterforskningsmetoder imidlertid komme på tale, hvor politiet iværksætter efterforskningsindsatsen før eller mens forbrydelsen begås, således f.eks. ved metoderne infiltration, lokkedue og agentvirksomhed.

I de senere år er iværksæt forskellige konkrete, overvågende tiltag, hvorfra politiet kan modtage data, der kan være relevante i strafforfølgende øjemed. Således ses

[6] Jf. Artikel 5: *"Politiets infiltration på digitale platforme – set i et menneskeretligt perspektiv"*, pkt. 5.

øget brug af tv-overvågning, f.eks. af broforbindelser (Storebæltsbroen), trafikknudepunkter (Limfjordstunnelen), foruden forskellige former for 'problemområder' (Jomfru Ane Gade i Aalborg, restaurationer, forskellige boligområder mv.), hvorfra der kan indhentes videooptagelser og data, der kan være relevante i efterforskningsmæssig sammenhæng. Andre tiltag i de senere år har mere karakter af strukturel, generel overvågning, såsom teleselskabernes lagring af data om telekommunikation, den såkaldte 'logningspligt', der blev indført i 2006, og som handler om, at teleselskaberne registrerer data om, hvem der ringer til hvem, hvornår og hvor længe og lagrer disse data i ét år, for at politiet kan få adgang til data, hvis det skulle blive nødvendigt som led i en strafferetlig efterforskning. Flere strukturelle, generelle overvågningsmekanismer er siden kommet til, således den automatiske nummerpladegenkendelse (ANPG),[7] samt det såkaldte PNR-register, som samler oplysninger om flypassagerer.[8] Med disse systemer har politiet fået en række nye data til rådighed, med forskellige restriktioner for politiets anvendelse. Således gælder som hovedregel krav om retskendelse ved indhentelse af loggede teledata fra teleselskaberne, mens politiet eksempelvis har umiddelbar adgang til data fra nummerpladegenkendelsen, der er reguleret ud fra sletning af 'hits' og 'no-hits'.

Dansk politi har en ambition om i videst muligt omfang at arbejde analyse- og videnbaseret (såkaldt "intelligence-led policing"), hvilket bl.a. har ført til indkøb og implementering af en analyseplatform (POLINTEL) fra den amerikanske virksomhed, Palantir, hvorved politiet fik et sammenhængende IT-system til bearbejdning og analyse af de store datamængder, der genereres både internt i politiet og som er tilgængelige fra eksterne datakilder.[9]

For at understøtte og sikre det retlige grundlag for analyseplatformen blev politiloven ændret, således at det nu følger af § 2 a, stk. 1, at politiet kan foretage tværgående informationsanalyser på grundlag af de oplysninger, politiet behandler, når det er nødvendigt af hensyn til udførelsen af politiets opgaver, jf. § 2.[10] Pol-Intel-systemet vil også kunne bruges til at forsøge at forudsige forbrydelser ved at udregne

[7] Jf. bekendtgørelse nr. 1776 af 16. december 2015 om politiets anvendelse af automatisk nummerpladegenkendelse (ANPG), senere erstattet af bekendtgørelse nr. 1080 af 20. september 2017, fastsat i medfør af politilovens § 2 a, stk. 3.

[8] Jf. Lov nr. 1706 af 27. december 2018 om indsamling, anvendelse og opbevaring af oplysninger om flypassagerer.

[9] Lovforslag nr. 171 af 29. marts 2017, pkt. 2.2.4. til en ændring af politiloven, jf. lov nr. 671 af 8. juni 2017 om politiets anvendelse af databaserede analyseredskaber og adgang til oplysninger om flypassagerer.

[10] Desuden er fastsat nærmere regler for politiets behandling af oplysninger i en række bekendtgørelser, således bekendtgørelse nr. 1076 af 20. september 2017 om ikrafttræden af § 1 i lov om ændring af lov om politiets virksomhed og toldloven, jf.

mønstre i kriminaliteten i bestemte områder, det såkaldte "predictive policing"; en metode, der ikke er taget i anvendelse i Danmark.[11]

2.3. Retsplejelovens regulering

Retsplejeloven afvejer hensynet til den enkelte borger og dennes privatliv over for hensynet til politiets kriminalitetsbekæmpelse ved i detaljer at anvise, hvornår og på hvilken måde politiet kan gøre indgreb i borgerens rettigheder og privatliv som led i en efterforskning. Loven indeholder en række almindelige bestemmelser om efterforskning, jf. kapitel 67 og 68, hvorefter følger en udførlig regulering af de 'straffeprocessuelle tvangsindgreb' i lovens kapitel 69-75 b.

Hans Gammeltoft-Hansen har defineret et straffeprocessuelt tvangsindgreb som "*en foranstaltning, der efter sit almindelige formål udføres som led i en strafforfølgning, og hvorved der realiseres en strafbar gerningsbeskrivelse rettet mod legeme, frihed, fred, ære eller privat ejendomsret*".[12] Et sådant tvangsindgreb kræver ifølge Gammeltoft-Hansen et klart hjemmelsgrundlag.[13]

Navnlig ved retsplejelovens regulering af de straffeprocessuelle tvangsindgreb træder afvejningen mellem hensynet til den enkelte over for hensynet til politiets efterforskning tydeligt frem. Således er der i reguleringen først og fremmest fastsat materielle betingelser for, hvornår indgreb kan iværksættes, i form af et kriminalitetskrav (i hvilke sager må indgrebet bruges), et mistankekrav (hvor sikre er politiet på, at det er den rette mistænkte, eller at en forbrydelse er ved at blive begået) og et indikationskrav (formålet med indgrebet). Dette suppleres af et proportionalitets-

---

lov nr. 671 af 8. juni 2017, bekendtgørelse nr. 1078 af 20 september 2017 om politiets behandling af oplysninger i forbindelse med tværgående informationsanalyser, bekendtgørelse nr. 1079 af 20. september om behandling af personoplysninger i Politiets Efterforskningsstøttedatabase (PED), samt bekendtgørelse nr. 1080 af 20. september 2017 om politiets anvendelse af automatisk nummerpladegenkendelse (ANPG).

[11] Mette Volquartzen: "Forskydninger mellem det private og det offentlige i smart politiarbejde", s. 171-189 i "*Ret SMART*", af Anita Rønne og Henrik Stevnsborg (red.), 2018. Se om "social media intelligence" (SOCMINT), "intelligence led policing" og "predictive policing", bl.a. Lilian Edwards og Lachlan Urquhart: "Privacy in Public Spaces: What Expectations of Privacy Do We Have in Social Media Intelligence?" (December 11, 2015). International Journal of Law and Information Technology (Autumn 2016) 24 (3), 279-310.

[12] Gammeltoft-Hansen: "*Straffeprocessuelle tvangsindgreb*", 1981, s. 44-45.

[13] Gammeltoft-Hansen: "*Straffeprocessuelle tvangsindgre*b", 1981, s. 23 ff.

princip, hvorefter politiets indgreb over for borgeren ikke må være mere indgribende, end formålet tilsiger.[14] Dette gælder både ved beslutningen om, hvorvidt tvangsindgrebet overhovedet skal iværksættes, og den nærmere udstrækning af indgrebet (omfang og varighed), og hvordan indgrebet konkret udføres over for borgeren.

Afvejningen mellem hensynet til den enkelte overfor hensynet til efterforskningen ses desuden i de processuelle betingelser for indgrebene, herunder hvorvidt politiet selv har kompetence til at beslutte indgrebet, eller om retten skal tillade indgrebet ved kendelse, ligesom der forekommer forskellige betingelser og begrænsninger for indgreb, eksempelvis i relation til varighed af indgrebet, underretning mv. Ved hemmelige indgreb ses en højere grad af beskyttelse af de berørte borgere, eksempelvis i form af beskikkelse af en indgrebsadvokat ved indgreb i meddelelseshemmeligheden, dataaflæsning og hemmelig ransagning.

Helt centralt for strafferetten og straffeprocessen er princippet om retssikkerhed, som overordnet set betyder en sikkerhed for, at retten sker fyldest.[15] Traditionelt forstås retssikkerhed som den enkelte borgers retssikkerhed over for vilkårlige overgreb fra staten,[16] og det er i den betydning begrebet anvendes i denne afhandling. Begrebet retssikkerhed er dog tillige anvendt i andre sammenhænge, bl.a. som beskyttelsen af samfundet og dets borgere mod det enkelte individ, hvor det sikres, at retten sker fyldest ud fra et samfunds- eller statsperspektiv.[17]

Som en del af det traditionelle, individorienterede retssikkerhedsbegreb kan der sondres mellem *procesretssikkerhed*, hvor der opstilles nogle retsgarantier til at

---

[14] Se eksempelvis proportionalitetsprincippet formuleret i retsplejelovens § 762, stk. 3, § 768 og § 768 a i tilknytning til varetægtsfængsling, i § 782, stk. 1 i tilknytning til indgreb i meddelelseshemmeligheden og i § 797 for ransagning.

[15] Trine Baumbach: *"Strafferet og menneskeret"*, 2014, s. 30 f. Om retssikkerhed, se endvidere Trine Baumbach: *"Det strafferetlige legalitetsprincip – hjemmel og fortolkning "*, 2008, s. 21 ff., Carsten Henrichsen: "Retssikkerhed – en begrebsanalyse", s. 309 f., og Steen Rønsholdt: "Om retssikkerhed og andre hensyn, s. 340, begge i "*Retlig polycentri*" af Peter Blume og Hanne Petersen (red.), 1993, Jørgen Dalberg-Larsen: "Hvad er retssikkerhed, og hvordan kan den fremmes", i "*Liv, arbejde og forvaltning*", af Peter Blume, Kirsten Ketscher og Steen Rønsholdt (red.), 1995, s. 121 f., Carsten Munk-Hansen: *"Retsvidenskabsteori"*, 2018, s. 235 f., Carsten Munk-Hansen: "Retssikkerhedshensynet", Kapitel 1 i *"Retssikkerhed i konkurrence med andre hensyn",* af Carsten Munk-Hansen og Trine Schultz (red.), 2012, Gorm Toftegaard Nielsen: "*Strafferet 1. Ansvaret*", 2013, s. 33 ff., og Michael Kistrup m.fl.: "*Straffeprocessen*", 2018, s. 22 f.

[16] Baumbach: *"Det strafferetlige legalitetsprincip"*, 2008, s. 22 ff.

[17] Baumbach: *"Det strafferetlige legalitetsprincip"*, 2008, s. 22 ff.

sikre, at en afgørelse får det materielt rigtige resultat, og *materiel retssikkerhed*, som angår en afgørelse eller doms hjemmel, og det strafferetlige legalitetsprincip skal ses som udtryk herfor, hvor borgeren skal kunne forudsige, hvad der udløser en strafferetlig sanktion.[18]

I forhold til den nye IT-kriminalitet udfordres retssikkerheden ved, at det ikke altid er muligt for borgeren at forudsige, hvad der er strafbart, jf. det strafferetlige legalitetsprincip i straffelovens § 1, når straffelovens bestemmelser er formuleret i forholdsvis brede vendinger, der skal sammenholdes med en mangfoldighed af nye digitale muligheder. Retssikkerheden udfordres også i en straffeprocessuel kontekst ved, at politiet har fået nye digitale efterforskningsmuligheder til rådighed, uden at disse metoder er udtrykkeligt reguleret i retsplejeloven. Dette kan indebære et – for borgeren ganske stort og vilkårligt – spillerum for politiets overvågning, indtrængen i privatlivet og indsamling af oplysninger.

3. Det straffeprocessuelle legalitetsprincip

De nye teknologiske muligheder udfordrer således den straffeprocessuelle regulering i retsplejeloven. Derudover aktualiserer disse nye værktøjer en generel problematik i relation til, hvordan det fastlægges, hvilke af politiets efterforskningsmetoder, der skal reguleres i retsplejeloven.

Udgangspunktet har hidtil været, at hvis metoden opfyldte Gammeltoft-Hansens definition af et straffeprocessuelt tvangsindgreb, hvorved der *"realiseredes en strafbar gerningsbeskrivelse rettet mod legeme, frihed, fred, ære eller privat ejendomsret"*[19], skulle metoden reguleres i retsplejeloven. Dette traditionelle, danske straffeprocessuelle udgangspunkt er nu under forandring som følge af retsudviklingen i relation til Den Europæiske Menneskerettighedskonvention. Særlig relevant er EMRK artikel 8, stk. 2, hvoraf følger, at indgreb i privatliv, familieliv, hjem og korrespondance kun må ske, hvis indgrebet er foreskrevet ved lov og er nødvendigt i et demokratisk samfund blandt andet af hensyn til at forebygge forbrydelser.[20]

Spørgsmålet om, hvilke efterforskningsværktøjer, der retligt skal reguleres, kan anskues som et "straffeprocessuelt legalitetsprincip", hvori må inddrages både danske straffeprocessuelle og menneskeretlige aspekter for at sikre den rette afvejning mellem hensynet til strafforfølgningen over for hensynet til de berørte borgere.

---

[18] Jf. Baumbach: *"Det strafferetlige legalitetsprincip"*, 2008, s. 23, og Carsten Henrichsen: "*Retssikkerhed og moderne forvaltning*", 1997, s. 83 ff.

[19] Gammeltoft-Hansen: "*Straffeprocessuelle tvangsindgreb*", 1981, s. 44-45, samt "Om afgrænsningen af 'straffeprocessuelle tvangsindgreb', U 1979B.1 ff.

[20] Jf. Artikel 4: "*Politiets hjemmel til 'hacking' som led i en efterforskning*", pkt. 2.

Kapitel 2 Afhandlingens formål

Det overordnede formål med denne artikelbaserede afhandling er at analysere den danske, retlige regulering af politiets hemmelige efterforskning på internettet. I afhandlingen undersøges det nærmere, hvordan den eksisterende retlige ramme bliver anvendt i forskellige efterforskningssituationer på internettet, og hvilke problematikker, den nuværende regulering rejser.

1. Problemformulering og centrale temaer

Når afhandlingens problemformulering er at analysere den danske, retlige regulering af politiets hemmelige efterforskning på internettet, skal her afklares de centrale begreber, der indgår heri.

Ved at anføre "på internettet" understreges, at det er politiets online-efterforskning, der er i fokus. Udtrykket 'digital efterforskning' kan forstås bredere ved også at omfatte de mere tekniske undersøgelser offline af eksempelvis computermateriel og tilbehør. Fokus for denne afhandling er således den online-efterforskning, der foregår her og nu (i "real-tid"), og som griber ind i borgerens privatliv og ejendom.

Betegnelsen "hemmelig efterforskning" fokuserer på de situationer, hvor politiet ikke legitimerer sig over for borgeren, når der anmodes om oplysninger eller indhentes beviser til brug for en straffesag. De retssikkerhedsmæssige betænkeligheder indtræder netop i disse situationer, hvor politiet hemmeligt skaffer sig adgang til borgerens data eller interagerer med borgeren under dække af at være en almindelig borger. I disse tilfælde mister borgeren rådigheden over sine data, og hvem de udleveres til, og politiet trænger sig ind på borgerens privatliv på en måde, hvor borgeren er uden mulighed for at kende de rette omstændigheder, med mulighed for kontradiktion, rense sig selv for skyld m.v.

I afhandlingen omfatter betegnelsen "IT-kriminalitet" de strafbare forhold, der enten foretages ved hjælp af IT (f.eks. databedrageri) eller som rettes mod IT-systemet selv ('hacking').[21] En række forbrydelser i straffeloven kan forekomme i både den fysiske verden og den digitale verden, således bedrageri, afpresning, deling af overgrebsbilleder og videoer, trusler mv. I denne afhandling betragtes sådanne forbrydelser som IT-kriminalitet, hvis de i den konkrete kontekst er begået ved hjælp af IT.

[21] Mads Bryde Andersen: *"IT-retten"*, 2005, s. 723.

Udtrykket "datasystem", som indgår i straffelovens § 263, bruges i afhandlingen synonymt med "informationssystem", som var det tidligere begreb i samme bestemmelse, og der var ved lovændringen i 2018 ikke tilsigtet nogen indholdsmæssig forskel.[22]

Under den overordnede ramme – politiets hemmelige efterforskning på internettet – er udvalgt to typetilfælde, som eksempler på politiets hemmelige efterforskningsmetoder. Den første type efterforskning omfatter politiets *'tekniske tvangsindgreb'*, hvorved politiet skaffer sig teknisk adgang til internettets datasystemer, servere, platforme mv. Den anden type efterforskning omfatter '*det menneskelige indgreb*', hvor politiet under dække interagerer med borgeren på internettet og dermed realiserer en eller flere af efterforskningsmetoderne infiltration, lokkedue og agentvirksomhed.

Disse to typetilfælde, som uddybes nedenfor, er udvalgt, fordi de sammen dækker hovedområdet for politiets hemmelige efterforskning på internettet, hvilket er det område, der er mest indgribende for borgerens privatliv og derfor rummer de største retssikkerhedsmæssige betænkeligheder.

Dertil kommer, at de to typer efterforskning er indbyrdes forbundne. Både politiets tekniske indgreb i et datasystem og det 'menneskelige indgreb', infiltration, hvor politiet under dække påvirker borgeren til at give politiet adgang til et privat datasystem, kan i realiteten give politiet hemmelig adgang til det samme: borgerens digitale privatliv.[23] Der er imidlertid markant forskel på reguleringen af de to typer efterforskning. Som det vil fremgå af afhandlingen, er politiets tekniske adgang til datasystemer restriktivt reguleret i retsplejeloven, mens politiets infiltration og påvirkning af borgeren ikke er reguleret. Ligeledes rummer de to hemmelige efterforskningsmetoder, lokkedue og agentvirksomhed, hvor politiet indtræder i og påvirker et kriminelt hændelsesforløb, en række retlige problematikker, der nærmere skal undersøges.

Analysen af reguleringen af politiets hemmelige efterforskning på internettet aktualiserer nogle overordnede temaer om det 'straffeprocessuelle legalitetsprincip' og definitionen af tvangsindgreb, som tidligere har været indgående diskuteret af Hans Gammeltoft-Hansen og Gorm Toftegaard Nielsen, og til en vis grad Birgitte Brøbech, men som ikke i de senere år har været genstand for nogen nyovervejelse. Denne

[22] Lov nr. 1719 af 27. december 2018 om ændring af straffeloven, retsplejeloven, lov om erstatningsansvar og medieansvarsloven (freds- og ærekrænkelser mv), trådt i kraft den 1. januar 2019, samt lovforslag nr. 20 af 3. oktober 2018, specielle bemærkninger til § 263, jf. nærmere herom i Del 3, Kapitel 2.
[23] Jf. Artikel 5: *"Politiets infiltration på digitale platforme – set i et menneskeretligt perspektiv"*, pkt. 3.3.

mere grundlæggende diskussion af, hvilke af politiets efterforskningsværktøjer, der skal lovreguleres, anskues i denne afhandling ud fra et digitalt perspektiv og navnlig i lyset af retsudviklingen i EMD' praksis, hvor praksis om indgreb i privatlivet mv., jf. EMRK artikel 8, fordrer regulering af flere efterforskningsværktøjer end traditionelt antaget i dansk straffeprocessuel teori.

I det følgende afsnit udmøntes problemformuleringen og de to typetilfælde af politiets hemmelige efterforskning på internettet til egentlige forskningsspørgsmål.

2. Forskningsspørgsmål

1. Hvordan er den retlige regulering af politiets hemmelige efterforskning på internettet?

    a. Hvordan er reguleringen af **'det tekniske tvangsindgreb'** på private områder på internettet? I den forbindelse inddrages straffelovens § 263 om 'hacking' som et udgangspunkt for, hvornår politiet er på 'offentligt' og 'privat' område på internettet.
    (ARTIKEL 1 om 'hacking')

        i. Hvilket anvendelsesområde har de straffeprocessuelle tvangsindgreb, og hvordan er samspillet imellem:
            1. Ransagning
            2. Indgreb i meddelelseshemmeligheden
            (ARTIKEL 2+3 om teledata og retsplejeloven)
            3. Dataaflæsning
            4. Observation

        ii. Er der noget teknisk indgreb, der ikke dækkes af retsplejelovens regulering?
        (*ARTIKEL 4 om politiets 'hacking'*).

    b. Hvordan er reguleringen af '**det menneskelige indgreb'**, hvor politiet interagerer med borgeren, under dække, med henblik på at få information, adgang til private områder ('hacking ved svig'), lokke gerningsmænd til en forbrydelse, afsløre en forbrydelse mv.

        i. Her vil indgå efterforskningsmetoderne infiltration, lokkedue og agentvirksomhed. *(ARTIKEL 5 om infiltration og ARTIKEL 6 om agentvirksomhed).*

2. Hvordan anskues **det straffeprocessuelle legalitetsprincip** og definitionen af det straffeprocessuelle tvangsindgreb i lyset af EMRK?

3. Afhandlingens struktur

Afhandlingen falder i fire dele. I denne Del 1 skitseres i det følgende en struktur for afhandlingen og de temaer og tidsskrifts-artikler 1-6, der indgår heri. Herefter følger i Kapitel 3 en redegørelse for de metodiske overvejelser i relation til afhandlingen.

Del 2 indeholder tidsskrifts-artiklerne 1-6, hvorefter Del 3 giver en samlet besvarelse af de stillede forskningsspørgsmål. Heri vil indgå en sammenfatning af artiklernes analyser samt videre perspektivering i forhold til de enkelte temaer. Del 4 indeholder en samlet, afsluttende perspektivering.

3.1. Politiets "tekniske tvangsindgreb"

Undersøgelsen af de retlige rammer for politiets hemmelige efterforskning på internettet, sker ved en analyse af politiets "tekniske indgreb". Hvorvidt der er tale om et indgreb, beror på, om politiet bevæger sig på offentligt tilgængeligt område og indsamler offentligt tilgængelige oplysninger, eller om der er tale om et indgreb i borgerens privatliv.

Politiet er i almindelighed berettiget til at gøre sig bekendt med, hvad der er offentligt tilgængeligt, hvilket nu udtrykkeligt fremgår af politilovens § 2 a, stk. 2,[24] som foreskriver, at indsamlingen og behandlingen af oplysninger fra offentligt tilgængelige kilder skal være nødvendig af hensyn til udførelsen af politiets opgaver efter politilovens § 2.

Den første relevante grænse for politiets hemmelige tekniske indgreb på internettet vil derfor kunne fastlægges ved at undersøge forskellen på 'privat' og 'offentligt' tilgængeligt område på internettet. Ved at se på 'hacking', som det er kriminaliseret for borgeren i straffelovens § 263, vil kunne udledes et bidrag til forståelsen af, hvornår der er tale om adgang til et privat område på internettet, idet en sådan adgang som udgangspunkt for politiet vil være at betragte som et tvangsindgreb, som skal ske efter retsplejelovens regler.

3.1.1. 'Hacking'-bestemmelsen i straffelovens § 263

I Artikel 1: *"'Hacking' og det digitale privatliv"*, analyseres straffelovens bestemmelse om at skaffes sig uberettiget adgang til andres oplysninger eller programmer i et informationssystem. Fokus i artiklen er på to typesituationer: Først den it-kyndige, der i egen opfattelse af hjælpsomhed tester sikkerheden ved et informationssystem, og hvor det diskuteres, hvornår en sådan teknisk påvirkning af systemet,

[24] Lov nr. 671 af 8. juni 2017, trådt i kraft den 22. september 2017 ved bekendtgørelse nr. 1076 af 20. september 2017. Endvidere gælder lov nr. 410 af 27. april 2017 om retshåndhævende myndigheders behandling af personoplysninger.

hvor man ikke har fået adgang til de egentlige data "inde i systemet", men alene adgang til den tekniske opsætning og administration af systemet, kan anses for 'hacking' efter § 263. Dernæst behandles de sociale medier som et nyt område for anvendelse af 'hacking'-bestemmelsen i lyset af U 2017.247 V. De sociale medier er kendetegnet ved mange forskellige 'zoner' af enten privat, offentlig eller halvoffentlig karakter, hvilket vanskeliggør fastlæggelsen af nogle egentlige rammer for 'hacking'-bestemmelsens anvendelse på dette område. Heri indgår spørgsmålet, om 'hacking' på de sociale medier kan ske på svigagtigt grundlag.

De to typesituationer i artiklen er udvalgt ud fra, at det også kunne være scenarier, som polititjenestemænd i en efterforskning blev sat i. I stedet for en IT-kyndig, der tester sikkerheden, kunne en polititjenestemand teste sikkerhedsforanstaltninger på informationssystemet for at se, om det var muligt at få adgang til siden, inden man anmoder om rettens kendelse til et sådant indgreb. Man kunne også forestille sig de sociale medier som et område, hvor politiet hemmeligt ville kunne indhente en mangfoldighed af private oplysninger.

Når fokus er lagt på disse to typesituationer, er der samtidig foretaget en vis nedprioritering af 'hacking'-sager, som relaterer sig til andre forhold, f.eks. ansættelsesforhold, enten som ansattes uberettigede adgang til hele eller dele af virksomhedens informationssystem, eller arbejdsgiverens uberettigede adgang til medarbejderens informationssystem, eksempelvis computer og iPad. Om end disse ansættelsesforhold spiller en forholdsvis stor rolle i forarbejderne til 'hacking'-bestemmelsen og i retspraksis, er den situation næppe relevant for politiet. Enten *har* politiet samtykke fra den samarbejdsvillige ejer af datasystemet, og får adgang til det, man skal bruge, eller også har man *ikke* samtykke, men vil i stedet gå hemmeligt til værks, hvilket nødvendiggør rettens kendelse til indgrebet, eller at politiet gør brug af infiltration til at få adgang til private datasystemer.

3.1.2. Hjemmel for politiets 'hacking'

Såfremt politiet ønsker at skaffe sig teknisk adgang til private data eller privat område på internettet, er der tale om et indgreb i borgerens privatliv, der kræver hjemmel i retsplejeloven. Dette følger af den traditionelle danske definition af straffeprocessuelle tvangsindgreb, som Hans Gammeltoft Hansen udarbejdede,[25] men følger også af EMRK artikel 8, hvilket fremgår af Artikel 4: *"Politiets hjemmel til 'hacking' som led i en efterforskning",* pkt. 2.

Der er ikke i retsplejeloven nogen udtrykkelig bestemmelse, som regulerer 'politiets hacking', forstået som det indgreb, hvor politiet uden samtykke skaffer sig adgang

[25] Jf. ovenfor, samt Gammeltoft-Hansen: "*Straffeprocessuelle tvangsindgreb*", 1981, s. 44-45.

til borgerens data i et informationssystem.[26] I stedet reguleres dette indgreb af reglerne om hemmelig ransagning, jf. § 799, dataaflæsning, jf. § 791 b og indgreb i meddelelseshemmeligheden, jf. § 780 ff. Centralt i vurderingen af lovhjemlen og samspillet mellem de tre tvangsindgreb ses U 2012.2614 H, hvor Højesteret tog stilling til politiets indgreb med rette kode i en mistænkts Facebook- og Messenger-profiler. Dette er en form for 'politi-hacking', som Højesteret – dog uden at anvende denne terminologi – vurderede, skulle anses som gentagen, hemmelig ransagning.

Samspillet mellem de tre tvangsindgreb – hemmelig ransagning, dataaflæsning og indgreb i meddelelseshemmeligheden – er undersøgt i en tidligere artikel.[27] Her blev påpeget det uhensigtsmæssige i, at disse tre indgreb, som ret beset kan give politiet adgang til de samme, digitale oplysninger, har forskelligt kriminalitetskrav: Hvor dataaflæsning og indgreb i meddelelseshemmeligheden kan ske i sager, hvor der kan straffes med mere end 6 års fængsel, er hemmelig ransagning forbeholdt ganske få alvorlige forbrydelser, såsom terror, drab, grov narkotikakriminalitet mv.

Indgreb i meddelelseshemmeligheden er særligt analyseret i to artikler: Artikel 2: *"Logning af teledata i lyset af Tele2-sagen"* og Artikel 3: "*Retsplejelovens regulering af politiets adgang til teledata"*. Inddragelsen af konteksten af teledata kræver en nærmere forklaring, som følger neden for i afsnit 3.1.3.

I Artikel 4: *"Politiets hjemmel til 'hacking' som led i en efterforskning"* samles deleelementerne fra disse artikler til en analyse af lovhjemlen og samspillet mellem de tre tvangsindgreb. I denne artikel behandles desuden den praktiske situation, hvor politiet ved beslaglæggelse af en computer eller en mobiltelefon, i realiteten får mulighed for at iværksætte et 'hacking'-indgreb, ved at etablere en fremadrettet, onlineovervågning af mails, chatfora, brugerprofiler på de sociale medier mv. Det undersøges, om et sådant indgreb er indeholdt i de meget milde regler om beslaglæggelse, eller om der i stedet realiseres en hemmelig ransagning.

I afhandlingens Del 3 vil analysen af politiets 'hacking'-hjemmel blive suppleret med en analyse af reglerne om observation, jf. retsplejelovens § 791 a, hvor det undersøges, om disse bestemmelser har et digitalt anvendelsesområde som led i politiets efterforskning på internettet. Observationsreglerne indeholder ikke en 'hacking'-hjemmel, men når først der er sikret adgang, kan observationsreglerne måske spille en rolle i forhold til, at politiet agerer *inde på* det private område ved f.eks. med software at 'trawle', 'udvinde' eller sortere data.

[26] Jf. Artikel 4: *"Politiets hjemmel til 'hacking' som led i en efterforskning"*, pkt. 1.
[27] Lene Wacher Lentz: "Hemmelig ransagning og brevstandsning i den digitale virkelighed", Juristen nr. 1/2016.

3.1.3. Kort om teledata

Under arbejdet med at analysere retsplejelovens regler om indgreb i meddelelseshemmeligheden var der i sommeren 2016 politiske tilkendegivelser om, at der ville blive fremsat et lovforslag om at genindføre den såkaldte "sessionslogning", hvorved brugernes internettrafik lagres hos teleudbyderne, herunder hvilke hjemmesider der besøges, således at politiet senere kunne få adgang til disse data til brug for en eventuel efterforskning. Sessionslogningen havde været i kraft i Danmark i perioden fra 2007 til 2014, hvor denne del af logningen blev ophævet i dansk ret, efter at EU-Domstolen i Digital Rights-sagen havde erklæret EU logningsdirektivet for ugyldigt.[28]

Logning af teledata, herunder den nugældende logning af brugerdata i relation til internetaktivitet, og derudover navnlig sessionslogning om brugeres præcise internetaktivitet, er relevant for politiets efterforskning på internettet, idet det herved reguleres, hvilke data der lagres og dermed vil være til rådighed for politiet.

I forhold til denne afhandlings forskningsspørgsmål blev logningen særlig relevant, da EU-domstolen den 21. december 2016 afsagde dom i "Tele2-sagen", hvor EU-Domstolen fandt, at den svenske logningspligt, som er meget lig den danske, var i strid med edata-direktivet og Chartrets bestemmelser. Dernæst kom EU-domstolen med anvisninger på, hvordan der kunne etableres en målrettet logning af teledata, og hvordan politiet måtte få adgang til disse lagrede data. Forudsætningen for begge var, at der var tale om forebyggelse eller bekæmpelse af grov kriminalitet. Ved også at tage stilling til politiets adgang til disse data, vil Tele2-sagen også have betydning for de danske regler i retsplejeloven om indgreb i meddelelseshemmeligheden.

I Artikel 2: *"Logning af teledata i lyset af Tele2-sagen"* analyseres den danske logningspligt[29] i forhold til Tele2-dommens konklusioner, hvorefter det undersøges, hvad der ligger i "grov kriminalitet", som efter Tele2-dommen nu er omdrejningspunktet for målrettet logning af teledata og politiets adgang til disse data. Artiklen skal ses som en nødvendig baggrundsartikel til Artikel 3: "*Retsplejelovens regulering af politiets adgang til teledata"*, hvor Tele2-dommens anvisninger sættes i forhold til den eksisterende regulering i retsplejeloven af indgreb i meddelelseshemmeligheden.

[28] EU-domstolens dom af 8. april 2014 i de forenede sager Digital Rights Ireland Ltd mod Minister for Communications, Marine and Natural Resources, Irland (sag C-293/12) og Kärntner Landesregierung (sag C-594/12), præjudiciel forelæggelse. Om sessionslogning, se Artikel 1: *"Logning af teledata i lyset af Tele 2-dommen"*, pkt. 4.
[29] Bekendtgørelse nr. 660 af 19. juni 2014, fastsat i medfør af retsplejelovens § 786, stk. 4.

I analysen af reglerne om indgreb i meddelelseshemmeligheden er inddraget denne aktuelle kontekst af logning, navnlig med tanke på, at logningsreglerne og formodentlig også retsplejelovens regler om indgreb i meddelelseshemmeligheden snart må forventes ændret i overensstemmelse hermed.[30] En analyse af de gældende bestemmelser om indgreb i meddelelseshemmeligheden uden at inddrage logningsproblematikken og Tele2-sagen ville forekomme mangelfuld.

3.2. Politiets 'menneskelige indgreb' på internettet

I de tilfælde hvor politiet interagerer med borgeren på internettet uden at give sig til kende, vil dette være omfattet af tre metoder, som i den danske straffeproces går under betegnelserne, infiltration, lokkedue og agentvirksomhed. De tre metoder blev beskrevet i Straffeprocesudvalgets Betænkning 1023/1984, og resultatet af dette arbejde og den efterfølgende politiske behandling blev, at alene agentvirksomhed blev reguleret i retsplejeloven, jf. § 754 a-e. Udgangspunktet var, at ingen af disse metoder udgjorde et straffeprocessuelt tvangsindgreb, da der ikke her "*realiseredes en strafbar gerningsbeskrivelse rettet mod legeme, frihed, fred, ære eller privat ejendomsret*", jf. Gammeltoft-Hansens definition, men udvalget fandt, at agentvirksomhed skulle undergives en regulering, da der var betænkeligheder forbundet med metoden.[31]

I forhold til den traditionelle opfattelse af, hvad der definerer et 'indgreb', jf. Gammeltoft-Hansens definition, kan denne afhandlings betegnelse 'menneskelige indgreb', måske terminologisk virke distraherende. Af hensyn til den videre systematik i afhandlingen er der imidlertid behov for en fælles betegnelse for de tre metoder,

[30] Status er pt., at revision af logningsreglerne er udskudt til folketingsåret 2018-19, jf. lov nr. 716 af 8. juni 2018. Ifølge lovforslag nr. 227 fremsat den 24. april 2019 var hensigten en udskydelse til næste folketingsår, men forslaget bortfaldt i forbindelse med folketingsvalget i juni 2019. Det kan konstateres, at Tele2-sagens konklusioner har givet anledning til adskillige retlige overvejelser, således fra dansk retspraksis, U 2019.2019 Ø, hvor landsretten afviste anmodning om at to teleselskaber skulle pålægges at udlevere teledata til ophavsrettighedshavere. En sådan situationen blev kort nævnt i Artikel 2: "*Logning af teledata i lyset af Tele2-sagen*", pkt. 3, navnlig note 31. Fra EU-Domstolens praksis, dom af 2. oktober 2018, i sag C-207/16, *Ministerio Fiscal* om indhentelse af brugerdata i en sag om røveri af mobiltelefon, samt *EU-Domstolens udtalelse 1/15* (Store afdeling) den 26. juli 2017 om aftale om overførsel af passageroplysninger mellem Canada og EU. Se endvidere artiklen: Anja Møller Pedersen, Henrik Udsen og Søren Sandfeld Jakobsen: "Data retention in Europe – the *Tele 2* case and beyond", International Data Privacy Law, 2018, Vol. 8, No. 2.

[31] Jf. hertil Artikel 5: *"Politiets infiltration på digitale platforme – set i et menneskeretligt perspektiv"*, pkt. 1 og 2, samt Artikel 6: *"Politiagenter i et menneskeretligt perspektiv",* pkt. 3, med henvisning til Bet. 1023/1984, s. 151 f. og Gammeltoft-Hansen: "Om afgræsningen af "straffeprocessuelle tvangsindgreb"", U 1979B.1, s. 15-16.

infiltration, lokkedue og agentvirksomhed, som er karakteriseret ved, at politiet under dække har kontakt til, interagerer med og eventuelt påvirker den enkelte borger. Desuden vil det senere fremgå, at Gammeltoft-Hansens definition af et straffeprocessuelt indgreb må siges at være under påvirkning af EMRK, hvor EMD i relation til artikel 8 anlægger et bredere perspektiv på, hvad der betragtes som 'indgreb' i privatlivet, korrespondance mv, jf. artikel 8, stk. 2.[32]

I Artikel 5: *"Politiets infiltration på digitale platforme – set i et menneskeretligt perspektiv"*, analyseres efterforskningsmetoden infiltration med udgangspunkt i 1984-Betænkningens beskrivelse, som angik infiltration i den fysiske verden. Herefter illustreres, hvordan infiltration kan foregå på digitale platforme, ligesom det påpeges, at både den tekniske 'hacking' og infiltration, hvor politiet påvirker borgeren til at tillade adgang, ret beset kan siges at være to forskellige måder for politiet at få adgang til samme datasystem. I artiklen inddrages endvidere et menneskeretligt perspektiv.

Endelig i Artikel 6 *"Politiagenter i et menneskeretligt perspektiv"* analyseres retsplejelovens regulering af politiets agentvirksomhed, hvor fokus navnlig er på den processuelle ramme for iværksættelse af agentvirksomhed. I artiklen inddrages to nylige danske straffesager, hvori har indgået ret spektakulære agentaktioner. Ligeledes inddrages et menneskeretligt perspektiv, idet EMD, der har fastsat en række retsgarantier for agentvirksomhed i medfør af EMRK artikel 6, stk. 1, har forholdt sig restriktivt til politiets gentagne eller fortløbende agentaktioner.

3.3. Det straffeprocessuelle legalitetsprincip

Disse nye tekniske og 'menneskelige' indgreb, der relaterer sig til internettets mange platforme, aktualiserer et traditionelt, straffeprocessuelt spørgsmål om, hvornår politiets efterforskningsmetoder skal reguleres i retsplejeloven. Temaet om dette "straffeprocessuelle legalitetsprincip" vil indgå løbende i hele afhandlingen, herunder også i artiklerne. I afhandlingens Del 3 sammenfattes og analyseres dette spørgsmål.

4. Afgrænsning

Når fokus er lagt på den hemmelige efterforskning på internettet, indebærer dette også visse, indledningsvise fravalg, som i det følgende gennemgås og begrundes.

De største retssikkerhedsmæssige betænkeligheder vurderes at være, når politiet teknisk eller ved menneskelig snilde, online gør indgreb i borgerens privatliv. Således vil ikke indgå i afhandlingen de tilfælde af digital efterforskning, der sker offline, f.eks. ved ransagning og undersøgelse af et USB-stik. Som naturlig forlængelse af

[32] Jf. Artikel 5: *"Politiets infiltration på digitale platforme – set i et menneskeretligt perspektiv"*, samt Del 3, Kapitel 1 om det straffeprocessuelle legalitetsprincip.

spørgsmål om ransagning hører normalt også et aspekt om beslaglæggelse. Bortset fra den helt konkrete problematik om online-fremadrettet overvågning ud fra beslaglagte computere og mobiltelefoner, som indgår i Artikel 4: *"Politiets hjemmel til 'hacking' som led i en efterforskning"*, inddrages i afhandlingen ikke yderligere aspekter om beslaglæggelse. Hvorvidt data kan beslaglægges og konfiskeres rummer interessante retlige problematikker, men fører for vidt at inddrage i denne fremstilling.

De europæiske databeskyttelsesregler med den europæiske forordning og den danske udmøntning er et stort, selvstændigt retsområde, og elementer herfra vil kun i begrænset, relevant omfang indgå i denne afhandling, der har et straffeprocessuelt perspektiv.

Desuden er der at nævne, at afhandlingen har fokus på politiets hemmelige efterforskning på internettet, hvorfor de danske efterretningstjenesters mulighed for hemmeligt at foretage indgreb, overvåge forskellige personer, aktiviteter og hjemmesider på internettet mv., ikke vil være en del af denne afhandling.

4.1. Internationale aspekter

Internettet er for os som brugere globalt og uden synlige grænser, og vi kan tilgå alle hjemmesider uden at bekymre os om, hvilket land hjemmesiden er henhørende i.[33] Dansk politi kan på samme måde tilgå offentligt tilgængelige danske og udenlandske hjemmesider,[34] men politiet er begrænset til kun at foretage indgreb og skaffe sig adgang til ikke-offentligt tilgængelige data på 'dansk territorium'. Dette beror grundlæggende på folkerettens princip om staternes suverænitet og ikke-indblanding i statens anliggender. Retstilstanden i dag er, at landegrænserne på internettet tegnes af, i hvilket land de konkrete servere befinder sig. Talrige er de spørgsmål og overvejelser, der rejser sig her, navnlig om det overhovedet giver mening at tale om landegrænser på internettet, og hvordan den straffeprocessuelle jurisdiktion i bund og grund bedst løses, så de nationale politimyndigheder ikke sættes skakmat ved, at de kriminelle bevæger sig frit rundt på hele internettet, og altså via talrige servere i forskellige lande og dermed henover forskellige landes kompetencer.

Særligt at bemærke er, at Højesteret i U 2012.2614 H tillod dansk politi at tilgå data på mistænktes Facebook og Messenger-brugerprofiler lagret på udenlandske servere, når data kunne tilgås med rette koder, uden at involvere udenlandske myndig-

[33] Afsnit 4.1. bygger på et uddrag af "Efterforskningens grænser på internettet", af Lene Wacher Lentz, s. 141 f., bidrag til antologien "*Eksponeret – Grænser for privatliv i en digital tid*", af Rikke Frank Jørgensen og Birgitte Kofod Olsen (red.), 2018.

[34] Se hertil Cybercrimekonventionens artikel 32 a, om Konventionen nærmere nedenfor i Kapitel 3.

heder. Hvordan Højesterets afgørelse stiller sig i forhold til folkeretten og andre landes straffeprocessuelle regler, vil bero på en større, international, folkeretlig analyse.[35] Disse aspekter omkring den straffeprocessuelle jurisdiktion har stor betydning for politiets operative, internationale efterforskning, men falder uden for rammerne af denne afhandling, som har fokus på dansk straffeproces og rammerne for dansk politi, og for forskningsspørgsmålene i denne afhandling er det ikke afgørende at inddrage dette internationale, jurisdiktionelle perspektiv.

[35] Højesterets konklusion, som i kendelsen ikke ses at indeholde nogen egentlige folkeretlige betragtninger, kan udlægges som et ret pragmatisk princip om, at "vi må, hvis vi kan", jf. Lars Bo Langsted: Commentary: commentary to Supreme Court Order U 2012.2614 H, Digital Evidence and Electronic Signature Law Review, 10 (2013), s. 164-165, og Jesper Løffler Nielsen: *"IT-retlige metaproblemer med retsplejeloven som praktisk studie"*, 2017, s. 208 ff. Se endvidere Lars Bo Langsted: "Efterforskning på udenlandske servere", Juristen nr. 3/2018, s. 94-98.

Kapitel 3 Metodiske overvejelser

1. Metode

I det følgende redegøres for de juridiske metoder, der anvendes i afhandlingens analyser. Afsnit 2 vil herefter indeholde en gennemgang af de retskilder og fortolkningsprincipper, der overordnet set er relevante for afhandlingen, det være sig dansk ret, EU-ret, Europarådets Cybercrimekonvention og Den Europæiske Menneskerettighedskonvention (EMRK).

1.1. Retsdogmatisk metode

Analysen af den retlige regulering af politiets hemmelige efterforskning på internettet vil tage sit udgangspunkt i den retsdogmatiske metode, hvor der ud fra de traditionelle retskilder, love, retspraksis mv. vil blive afklaret, hvad der er gældende ret.[36] Heri vil indgå danske retskilder, foruden retskilder, der hidrører fra det EU-retlige samarbejde og fra Europarådets samarbejde om Cybercrimekonventionen og Den Europæiske Menneskerettighedskonvention.

Som følge af den hastige teknologiske udvikling er den danske retsudvikling for de straffeprocessuelle tvangsindgreb, der er relevante for den digitale efterforskning, sket sporadisk og ujævnt over tid, hvorfor der i analysen vil være et særligt fokus på den samlede systematik og sammenhængen i reguleringen af tvangsindgrebene, navnlig hvor brudfladerne mellem de relevante tvangsindgreb og samspillet mellem bestemmelserne synes uhensigtsmæssige. Derudover er i afhandlingen et særligt blik på samspillet mellem de lovregulerede og ulovregulerede efterforskningsmetoder. Dette vurderende og kritiske blik på den gældende retlige regulering er indeholdt i den retsdogmatiske metode.[37]

1.2. Internettet og retlig pluralisme

Når man skal forholde sig til reguleringen af politiets efterforskning på internettet, er det værd at holde sig for øje, at uanset om den strafbare handling og politiets efterforskning kan siges konkret at være underlagt dansk jurisdiktion og dermed dansk lovgivning, er internettet et særligt retligt område, der i vidt omfang udvikles

---

[36] Christina D. Tvarnø og Ruth Nielsen: *"Retskilder og retsteorier*", 2017, s. 29 f., Carsten Munk-Hansen: *"Retsvidenskabsteori"*, 2018, s. 64 ff. og 204 ff., Peter Blume: *"Juridisk metodelære"*, 2009, s. 161, Peter Blume: *"Retssystemet og juridisk metode"*, 2016, s. 40, Jens Evald og Sten Schaumburg-Müller: *"Retsfilosofi, retsvidenskab og retskildelære"*, 2004, s. 207 og 212 ff.

[37] Jens Evald og Sten Schaumburg-Müller: *"Retsfilosofi, retsvidenskab og retskildelære"*, 2004, s. 207 og 231 ff., og Sten Schaumburg-Müller: *"Fem retsfilosofiske teser"*, 2009, s. 410 ff.

og styres af private, kommercielle aktører, og i mindre grad af de enkelte nationale myndigheder. Dette ses eksempelvis ved, at brugerne agerer på udenlandske hjemmesider, der for det første er underlagt andre landes jurisdiktion og lovgivning, og for det andet er brugerens aktivitet reguleret af det aftaleforhold, man indgår med den konkrete hjemmeside/platform.[38]

Der er ikke en egentlig, samlet, international regulering af internettet, som i stedet kan siges at være kendetegnet ved en retlig pluralisme, hvor regulering og normer i bred forstand udgår fra en række forskelligartede aktører, såsom nationale myndigheder, internationale institutioner, private kommercielle aktører og brugerne selv. Retlig pluralisme er af Jørgen Dalberg-Larsen beskrevet som *"en flerhed af retsordener eller retsnormer af forskellig art, som dækker det samme område".*[39] Begrebet har derudover været omfattende diskuteret både i dansk og international sammenhæng ud fra forskellige juridiske, antropologiske og sociale perspektiver.[40] I denne afhandling vil ikke ske en begrebsudvikling af retlig pluralisme i forhold til internettet som retligt fænomen i et strafforfølgende og retshåndhævende perspektiv. Formålet er alene deskriptivt; at beskrive den særlige kontekst, som internettet udgør som område for politiets efterforskningsindsats.

Når der ikke for internettets mange datasystemer og platforme gælder nogen egentlige, samlede retlige standarder, der er underlagt myndighedernes kompetence og kontrol, aktualiseres en række problematikker for staten, der ønsker at regulere borgerens adfærd på internettet, sikre visse grundlæggende rettigheder for borgerens

[38] De nærmere omstændigheder ved dette aftaleforhold er beskrevet i Artikel 1: *"'Hacking og det digitale privatliv"*, pkt. 5.

[39] Jørgen Dalberg-Larsen: *"Rettens enhed – en illusion? Om retlig pluralisme i teorien og i praksis"*, 1994, s. 43.

[40] Om retlig pluralisme se endvidere Jørgen Dalberg-Larsen: "Nogle bemærkninger om begrebet retlig pluralisme", i "*Ikke kun retsfilosofi – Festskrift til Sten Schaumburg –Müller*", af Nis Jul Clausen m.fl. (red.), 2016, Hanne Petersen: "Globalisering og retspluralisme – Juridiske begreber i forandring" og Sten Schaumburg-Müller: "Kritik af den rene retspluralisme" begge i "*Retlig mangfoldighed – En fælles udfordring for retsvidenskab og antropologi*" af Sten Schaumburg-Müller & Bodil Selmer (red.), 2003, henholdsvis s. 15 og s. 45, Jens Evald og Sten Schaumburg-Müller: "*Retsfilosofi, retsvidenskab & retskildelære*", 2004, s. 285 ff., og Carsten Munk-Hansen: "*Retsvidenskabsteori*", 2018, s. 181 ff. og s. 380 ff. Af international litteratur se bl.a.: Sally Falk Moore: *"Law as a Process"*, New York, 1978, John Griffiths: "What is Legal Pluralism" i Journal of Legal Pluralism, (1986) 24: 1-55, Sally Engle Marry: "Legal Pluralism" i Law & Society Review, Vol. 22, No. 5 (1988), pp. 869-896, samt Gunther Teubner: "Global Bukowina: Legal Pluralism in the World-Society" i "*Global Law Without a State*" af Gunther Teubner (ed.), Dartsmouth, pp. 3-28, 1996.

kommunikation på internettet og håndhæve og sanktionere uhensigtsmæssig adfærd fra borgere og virksomheder.

De nationale myndigheder har vanskeligt ved at regulere og håndhæve, hvad der foregår på internettet, og myndighedernes ageren er i vidt omfang begrænset til at henstille til kommercielle systemudbydere om at iværksætte forskellige tiltag for at dæmme op for brugernes uhensigtsmæssige adfærd mv. Et nyligt eksempel er EU-ekspertgruppen om misinformation, som i samarbejde med en række sociale medier, bl.a. Google, Facebook og Twitter, i september 2018 enedes om et "Code of Practices".[41] Her forpligter parterne sig til at iværksætte en lang række tiltag mod misinformation, herunder at lukke falske profiler, og at udvikle teknologier til at identificere misinformation.[42]

Som et dansk eksempel på forsøg på regulering kan nævnes en ændring af retsplejeloven i 2017, hvor der i § 791 d blev indsat en hjemmel til blokering af hjemmesider efter retskendelse, hvis der er grund til at antage at der fra hjemmesiden begås en overtrædelse af straffelovens §§ 114-114 i, § 119 eller § 119 a, og blokeringen ikke står i misforhold til sagens betydning og den ulempe, indgrebet må antages at medføre.[43] Det fremgår af lovforslaget,[44] at der siden 2005 i Danmark er sket blokering af hjemmesider på aftalebaseret grundlag med en række internetudbydere (bl.a. DK Hostmaster, der står bag .dk-hjemmesider) i et samarbejde, der betegnes Netfilterordningen, hvor Rigspolitiet i samarbejde med Red Barnet og størstedelen af de danske internetudbyderne forsøger at forhindre adgang til hjemmesider, hvor der findes materiale vedrørende seksuelt misbrug af børn. Når Rigspolitiet får kendskab til en sådan hjemmeside, videregives oplysninger om siden til internetudbyderne, der herefter iværksætter en såkaldt DNS-blokering af hjemmesiden. Blokeringen vil medføre, at forsøg på at tilgå hjemmesiden vil blive mødt med en besked om at adgangen er blokeret, fordi siden indeholder materiale omfattet af straffelovens § 235. Videre fremgår det imidlertid af lovforslaget, at det er muligt at omgå en sådan blokering for en person med en vis teknisk indsigt. Tiden vil vise, om den nye hjemmel til blokering i retsplejelovens § 791 d vil blive brugt, og hvor effektiv en sådan blokering vil være.

De private systemudbyderes store selvbestemmelse og råderum på internettet kan eksemplificeres ved et utilsigtet læk i foråret 2017, hvorved Facebooks retningslinjer for moderering kom til offentlighedens kendskab, således hvilke ytringer, billeder,

[41] LINK: https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation

[42] Søren Sandfeld Jakobsen: "Misinformation ("fake news") i retlig belysning", Juristen 1/2019, pkt. 7.

[43] Lov nr. 674 af 8. juni 2017.

[44] Herom i det følgende fra lovforslag nr. 192 af 26. april 2017, pkt. 3.1.1.

videoer og streaming, der fjernes af Facebooks ca. 4.500 moderatorer af hensyn til stødende indhold.[45] Andre platforme er næsten fuldstændig brugerdrevne, eksempelvis Jodel-platformen, hvor brugere inden for et afgrænset geografisk område, i anonymitet kan skrive udsagn på siden, der er tilgængelig for andre i området. Det er muligt for brugere ved intensiv brug af platformen at opnå moderator-status til at fjerne og ændre andre brugeres indlæg.

Én sag er reguleringen af brugernes uhensigtsmæssige adfærd på internettet og systemudbydernes rolle og samarbejde med myndighederne i den forbindelse, en anden sag er at beskytte brugernes privatliv over for systemudbyderne, der har en kommerciel interesse i at indsamle, samkøre og udvinde viden fra brugernes private data. I lyset af Cambridge Analytica-sagen står det klart, at der er et stort spillerum og et kommercielt marked for private, digitale aktører i at udnytte indsamlingen af data, og at denne omfattende dataindsamling kan få betydning for demokratiet ved at påvirke valghandlinger, folkeafstemninger mv. I EU-regi skal den europæiske databeskyttelsesforordning (GDPR) ses som et vigtigt tiltag i den sammenhæng, og ligeså vel EU-kommissionens opgør med de store systemudbydere på det digitale marked med udstedelse af anselige bøder efter konkurrencelovgivningen.

I forhold til afhandlingens temaer må denne retlige pluralisme stå som en vigtig kontekst, først og fremmest fordi borgeren som udgangspunkt agerer på kommercielle, internationale platforme. Dernæst fordi alle forslag til forbedringer af politiets efterforskningsmuligheder skal ses i lyset af, internettet er et område, hvor nationale kontrol- og håndhævelsesmuligheder kan være meget begrænsede. Man må i vidt omfang erkende, at "hertil og ikke meget længere" kan man komme ved national lovgivning og politimyndighed.

Denne kontekst er særlig vigtig ved de 'menneskelige indgreb', infiltration, lokkedue og agentvirksomhed, når interaktionen med borgeren foregår på internettets digitale platforme. Her må politiet gøre sig nogle strategiske overvejelser i hvilket omfang, platformen skal inddrages eller orienteres om den hemmelige efterforskning, der er iværksat, jf. nærmere nedenfor i Del 2, kapitel 4.

Helt konkret i forbindelse med udarbejdelsen af Artikel 5: *"Politiets infiltration på digitale platforme - set i et menneskeretligt perspektiv"*, ville det være interessant at få kendskab til Facebooks holdning til de tilfælde, hvor politiet måtte anvende en falsk profil til infiltration. Facebooks' privatlivspolitik og vilkår mv. gav intet svar

[45]Om Facebooks moderering, se Peter Blume: "Privat censur", Juristen, nr. 1/2017. s. 3, endvidere fra dagspressen, LINK: http://nyheder.tv2.dk/udland/2017-05-22-facebooks-hemmelige-regler-laekket?cid=tv2.dk:Facebooks hemmelige regler lækket:article og LINK:http://nyheder.tv2.dk/udland/2017-05-22-laekkede-dokumenter-afsloerer-facebooks-politik-for-moderering-kun-en-broekdel

herpå, og en forespørgsel til Facebook af 15. januar 2019 (bilag 1) og en opfølgende rykker af 3. juni 2019 er fortsat ubesvaret. Hvor de danske offentlige institutioner traditionelt har været hierarkisk opbygget, retligt normeret og i vidt omfang åben for offentlighedens indsigt i procedurer og retningslinjer, er der nu på vigtige områder af vores digitale, daglige liv, nogle kommercielle og i vidt omfang udenlandske, aktører, som ikke nødvendigvis har nogen interesse i at give indsigt i forretningsgange og prioriteringer.

1.3. Retspolitiske betragtninger og friere overvejelser

Afhandlingens overordnede metode er retsdogmatisk. Dog er der i tilknytning til de retsdogmatiske konklusioner, hvor der påpeges problematiske aspekter for retsanvendelsen og kritik af den retlige regulering, valgt en konstruktiv tilgang og opfølgning. Således vil disse kritiske konklusioner blive efterfulgt af en række betragtninger af mere retspolitisk karakter. Dette kan være enten i form af forslag til ændret retsanvendelse (de lege sententia ferenda) eksempelvis ved opfordring til øget fokus på at inddrage menneskeretlige retsgarantier ved afgørelsen af konkrete sager, eller der kan være tale om egentlige retspolitiske betragtninger med opfordringer til at ændre den retlige regulering (de lege ferenda), eksempelvis ved straffelovens 'hacking'-bestemmelse eller retsplejelovens regulering af politiets indgrebshjemler.[46]

I denne konstruktive opfølgning på afhandlingens konklusioner vil også indgå friere overvejelser, eksempelvis ud fra retsplejelovens og straffesystemets sammenhængende systematik, ligesom der også vil ske inddragelse af grundlæggende principper på straffesystemets område, objektivitetsprincippet, den materielle sandheds princip, proportionalitetsprincippet mv.

1.4. Komparativ metode

Afhandlingen indeholder ikke en egentlig komparativ analyse i den forstand, at den danske regulering analyseres i forhold til et andet lands regulering. I afhandlingens forskellige dele vil den retlige regulering fra EMRK og EMD – og i mindre omfang EU-ret – blive inddraget, således i Artikel 2: "*Logning af teledata i lyset af Tele2-dommen*", som indeholder et mindre, afgrænset komparativt element. Dette beror på, at EU-Domstolen i Tele2 dommen tog stilling til præjudicielle søgsmål fra en svensk og en engelsk domstol, og dermed angik Domstolens udtalelser først og fremmest disse to landes reguleringer i forhold til logning mv. Som anført i Artikel 2: "*Logning af teledata i lyset af Tele2-dommen*", er der i vidt omfang overensstemmelse mellem

[46] Om de lege ferenda og de lege sententia ferenda, se Alf Ross: "*Ret og retfærdighed En indførelse i den analytiske retsfilosofi*", 1966, Nyt Nordisk Forlag Arnold Busck, s. 60, 119 og 170, Christina D. Tvarnø og Ruth Nielsen: *"Retskilder og retsteorier"*, 2017, s. 30 og 445 f., Jesper Løffler Nielsen: *"IT-retlige metaproblemer med retsplejen som praktisk studie"*, 2017, s. 62 ff., samt Carsten Munk-Hansen: *"Retsvidenskabsteori"*, 2018, s. 75 og 214 f.

den svenske logningsregulering, som EU-Domstolen tog stilling til, og den danske logningspligt, hvorfor Tele2-dommen i høj grad har betydning for dansk ret.

Retspraksis fra EU-Domstolen og Den Europæiske Menneskerettighedsdomstol er i bund og grund stillingtagen til de enkelte staters retlige regulering i forhold til de EU-retlige eller menneskeretlige standarder. Når denne retspraksis indgår i afhandlingens analyser, inddrages dog ikke den nationale, retlige regulering i en komparativ kontekst. I analysen inddrages alene de udtalelser og fortolkninger, Domstolene anlægger i relation til retlige instrumenter, der også er gældende for dansk ret. Det være sig telelovgivningen og Charteret i relation til EU, og de enkelte rettigheder i Den Europæiske Menneskerettighedskonvention, som de fortolkes af Den Europæiske Menneskerettighedsdomstol.

2. Retskilder og fortolkningsprincipper

I det følgende redegøres i hovedtræk for de retskilder, som inddrages i afhandlingen, hvor der behandles danske retskilder, EU-retlige retskilder samt retskilder fra det mellemstatslige samarbejde under Europarådet, hvor Cybercrimekonventionen og Den Europæiske Menneskerettighedskonvention på hver sin måde er blevet en del af dansk ret. Disse forskelligartede retskilder har følgelig hver sin retlige kontekst og derfor også egne særlige fortolkningsprincipper.

2.1. Danske retskilder

For den retsdogmatiske analyse af den danske regulering er de traditionelle retskilder relevante, love, bekendtgørelser og i den forbindelse forarbejder og betænkninger for at se formålet med – og sammenhængen i – reguleringen, foruden retspraksis for at undersøge, hvordan reguleringen fortolkes og anvendes i konkrete sager.

Særligt vil indgå retsplejelovens bestemmelser, der regulerer politiets efterforskning og ageren over for borgeren. Helt central for reguleringen af de straffeprocessuelle tvangsindgreb er Strafferetsplejeudvalgets Betænkning 1023/1984, der danner grundlag for de regler om indgreb i meddelelseshemmeligheden og agentvirksomhed, som med senere ændringer, fortsat er gældende.

I forhold til udviklingen af straffelovens regulering af datakriminalitet er Straffelovrådets Betænkning 1032/1985 relevant, idet Straffelovrådet udover generelt at forholde sig til datateknikken i forhold til forbrydelserne tyveri, hærværk, brugstyveri og underslæb, også tog stilling til bl.a. den uberettigede indsigt i data, hvilket dannede grundlag for 'hacking'-bestemmelsen i straffelovens § 263.

I 1997 nedsatte Justitsministeriet et udvalg om økonomisk kriminalitet og datakriminalitet ("Brydensholt-udvalget"), der i årene 1999-2004 afgav 11 betænkninger om en række emner med relation til økonomisk kriminalitet og datakriminalitet. Af disse

skal her fremhæves tre af udvalgets betænkninger: Betænkning 1371/1999 om udviklingen i lovgivningen og kriminaliteten samt hæleri og anden efterfølgende medvirken, Betænkning 1377/1999 om børnepornografi og IT-efterforskning, som bl.a. reviderede reglerne om indgreb i meddelelseshemmeligheden, samt Betænkning 1417/2002, der udover at behandle visse almene problemstillinger vedrørende IT-kriminalitet, også dannede grundlag for senere kriminalisering af bl.a. uretmæssig besiddelse og anvendelse af adgangsmidler (betalingskortoplysninger, adgangskoder mv.)

Udover retsplejeloven og straffeloven er politiloven aktuel at inddrage, idet politiloven overordnet fastlægger politiets opgaver inden for og uden for strafferetsplejen.[47] Politilovens § 16 indeholder en række principper, der gælder generelt for politiets magtanvendelse, dvs. både inden for og uden for straffeprocessen, og som Ib Henricsson sammenfatter i et "krav om nødvendigheden af indgrebet", at indgrebet er det "mindst indgribende og tilstrækkelige middel", et "krav om proportionalitet mellem mål og middel", samt at selve indgrebet udføres så "skånsomt som omstændighederne tillader, så eventuelle skader begrænses."[48]

Med hjemmel i politiloven udfører politiet en række operationelle aktiviteter af ikkeretlig karakter, som i den forvaltningsretlige terminologi betegnes faktisk forvaltningsvirksomhed. Her suppleres politilovens regulering af de almindelige forvaltningsretlige principper, som i øvrigt gælder for alt, hvad politi og anklagemyndighed foretager sig, således forbuddet mod magtmisbrug, og at dét man som forvaltningsmyndighed foretager sig over for borgeren skal være sagligt begrundet og ikke må gå videre end formålet tilsiger (proportionalitetsprincippet) mv.[49]

Som belysning af, hvordan myndighedspersoner agerer over for borgeren, indeholder udtalelser fra Folketingets Ombudsmand en række normer for god forvaltningsskik. Dette inddrages i afhandlingen i forhold til infiltration af digitale platforme, hvor Ombudsmanden i afgørelsen, FOB 2011.1501, tog stilling til en skattemedarbejders indhentelse af oplysninger fra en borgers Facebook-profil.

Navnlig i forhold til teledata og indgreb i meddelelseshemmeligheden vil reguleringen af teleudbyderne (teleloven mv.) og den almindelige persondataret i et vist omfang blive inddraget.

[47] Lov nr. 956 af 20. august 2015 om politiets virksomhed.
[48] Ib Henricson: *"Politiret"*, 2016, s. 252 ff.
[49] Om faktisk forvaltningsvirksomhed, se bl.a. Ib Henricson: *"Politiret"*, 2016, s. 228, Sten Bønsing: "*Almindelig forvaltningsret*", 2018, s. 90 f., samt Karsten Revsbech m. fl.: "*Forvaltningsret. Almindelige emner*", 2016, s. 104 ff.

I forhold til databeskyttelse og borgerens rettigheder i den henseende, må her nævnes retshåndhævelsesloven, jf. lov nr. 410 af 27. april 2017 om Retshåndhævende myndigheders behandling af personoplysninger, som er en gennemførelse af Europa-Parlamentets og Rådets direktiv (EU) 2016/680 af 27. april 2017, se neden for om EU-retskilder.

2.1.1. Danske fortolkningsprincipper

Udgangspunktet er den retsdogmatiske metode, hvor retskilder analyseres efter almindeligt gældende retsprincipper for at fastslå, hvad der er gældende ret. Her vil i udgangspunktet ske en ordlydsfortolkning af de konkrete bestemmelser suppleret med en analyse af forarbejder (motivfortolkning) for at finde formål med bestemmelserne og en sammenhæng med andre tilgrænsende områder.[50] Endvidere inddrages retspraksis som udtryk for fortolkning af retskilder, hvori indgår overvejelser om, hvorvidt retspraksis fastlægger en ny retstilstand (præjudikat).[51]

Særligt inden for strafferetten er spørgsmålet, i hvilket omfang straffebestemmelser kan fortolkes udvidende (analogi), jf. det strafferetlige legalitetsprincip i straffelovens § 1 og legalitetskravet i EMRK artikel 7, stk. 1. Dette aspekt om analogi uddybes senere i afhandlingens Del 3, hvor analogi først inddrages i analysen af det strafferetlige legalitetsprincip, og senere i relation til 'hacking'-bestemmelsen og det strafferetlige legalitetsprincip.

2.1.2. Litteratur – "State of the art"

Der ses ikke nogen samlet videnskabelig behandling af denne afhandlings temaer relateret til politiets hemmelige efterforskning på internettet, hvor den tekniske adgang og den menneskelige adgang undersøges, og der gives et samlet kritisk blik på denne retstilstand.

Det digitale aspekt ved politiets efterforskning ses kun fragmenteret behandlet. Særlig relevant for afhandlingens temaer er to artikler af Lasse Lund Madsen, som har behandlet aspekter relateret til politiets digitale efterforskning, således om agentvirksomhed på digitale platforme i artiklen: "Agentvirksomhed online – efterforskning i IT-relaterede sager om misbrug af børn" i U 2017B.95. Derudover om edition

[50] Christina D. Tvarnø og Ruth Nielsen: *"Retskilder og retsteorier"*, 2017, s. 29 f. og 243 ff., Carsten Munk-Hansen: *"Retsvidenskabsteori"*, 2. udgave, 2018, s. 297 ff., Peter Blume: *"Retssystemet og juridisk metode"*, 3. udgave, 2016, s. 208 ff., samt Mads Bryde Andersen: *"Ret & Metode"*, 2002, s. 169 ff.

[51] Carsten Munk-Hansen: *"Retsvidenskabsteori"*, 2. udgave, 2018, s. 320 ff., Jens Evald og Sten Schaumburg-Müller: *"Retsfilosofi, retsvidenskab og retskildelære"*, 2004, s. 298 ff., Peter Blume: *"Retssystemet og juridisk metode"*, 3. udgave, 2016, s. 245 ff., samt Mads Bryde Andersen: *"Ret & Metode"*, 2002, s. 154 f.

i artiklen: "Edition som efterforskningsmiddel – med særligt henblik på internetrelaterede bedragerisager", U 2017B.205. Relateret til 'hacking', dog som borgerens strafansvar, har Helena Lybæk Guðmundsdóttir analyseret straffelovens § 263 i ph.d.-afhandlingen, *"Clarifying broad hacking statutes"*, Aalborg Universitet, 2015. Som et internationalt perspektiv for politiets efterforskning, ses Lars Bo Langsteds artikel: "Efterforskning på udenlandske servere", Juristen nr. 3/2018, s. 94-98.

En samlet analyse af reguleringen af politiets hemmelige efterforskning på internettet vil fastlægge gældende ret, og hvordan afvejningen sker mellem de grundlæggende straffeprocessuelle hensyn til politiets kriminalitetsbekæmpelse overfor hensynet til borgerens privatliv, ligesom det afdækkes hvordan retstilstanden tilgodeser borgerens retssikkerhed. På baggrund af denne analyse påpeges en række uhensigtsmæssigheder i den gældende retstilstand. Afhandlingens gennemgående tema om, hvilke efterforskningsmetoder, der kræver regulering i retsplejeloven, tager udgangspunkt i Gammeltoft-Hansens definition af et tvangsindgreb og kritikken heraf, hvorefter dette "straffeprocessuelle legalitetsprincip" genovervejes i lyset af nye digitale og menneskeretlige perspektiver.

2.2. EU-rettens betydning for dansk strafferet og straffeproces

Her skal kort redegøres for EU-rettens betydning for den danske strafferet og straffeproces, idet spørgsmålet er relevant i forhold til, i hvilket omfang EU-retlige kilder skal inddrages i afhandlingens analyser.

Den danske strafferet og straffeproces er i sit udgangspunkt nationalt reguleret, hvilket følger af det danske retsforbehold.[52] Danmark har tidligere i vidt omfang deltaget i EU-samarbejdet om retlige og indre anliggender i "Søjle 3-samarbejdet" på mellemstatsligt grundlag, hvilket medførte en række af de såkaldte Rammeafgørelser, der blev implementeret i dansk ret.[53] Ved Lissabon-traktatens ikrafttræden i 2009 blev EU-samarbejdet flyttet til det overstatslige samarbejde, og det tidligere mellemstatslige samarbejde ophørte, dog således at rammeafgørelserne – og samarbejde baseret herpå – fortsat er i kraft. Danmark deltager ikke i det overstatslige samarbejde og dermed ikke i vedtagelsen af foranstaltninger om det retlige samarbejde i straffesager og politisamarbejdet efter TEUF art. 82-89, ligesom ingen af de

[52] Maastricht-traktaten og det nationale kompromis samt Protokol nr. 22 om Danmarks stilling. Se hertil Thomas Elholm: "Det retlige forbehold og strafferetten" i "*EU-retten i Danmark*", af Birgitte Egelund Olsen og Karsten Engsig Sørensen (red.), 2018, s. 87-104.

[53] Eksempelvis Rådets rammeafgørelse 2002/475/RIA af 13. juni 2002 om bekæmpelse af terrorisme og Rådets rammeafgørelse 2002/584/RIA af 13. juni 2002 om den europæiske arrestordre.

foranstaltninger, der er vedtaget i henhold til disse bestemmelser er bindende for eller finder anvendelse i Danmark.[54]

Dog modificeres udgangspunktet om ren dansk regulering af strafferetten og straffeprocessen af navnlig tre forhold, som kort skitseres i det følgende.

For det første at en del af den danske strafferegulering udgøres af den såkaldte særlovgivning inden for sektorer som miljø, dyrevelfærd og transport mv., som på EU-plan indeholder ganske mange detaljerede materielle normer. Her overlades det til medlemslandene at fastsætte passende foranstaltninger for overtrædelse af disse normer, men det er EU-domstolen, der endeligt fastlægger indholdet og gyldigheden af EU-reglerne, og danske domstole skal i en straffesag fortolke EU-reglerne på samme måde som EU-domstolen.[55]

For det andet, at Danmark efter Lissabon-traktatens ikrafttræden nu kan 'vælge' ad hoc at tage den EU-retlige regulering til sig, og dermed alligevel sikre at der er overensstemmelse mellem dansk lovgivning og de øvrige medlemslandes regulering, forudsat der ikke er tale om gensidig anerkendelse eller gensidig udveksling af oplysninger mv., som kræver en egentlig parallelaftale.[56]

To eksempler på sådan 'tilegnelse' af EU-strafferetlige standarder skal nævnes: Første eksempel angår en ændring i 2012 af straffelovens § 262 a (om menneskehandel), hvorved der sikredes overensstemmelse med et europæisk direktiv på området, hvilket krævede en dansk lovændring i forhold til strafferammen og den danske

[54] Som anført af Baumbach i "Strafferetten og EU" i "*Retskildernes kamp – Forholdet mellem national offentlig ret og udefra kommende ret*" af Trine Baumbach og Peter Blume (red.), 2012, s. 57. Dette følger af artikel 1 og 2 i Protokol nr. 22 om Danmarks stilling.

[55] Baumbach: "Strafferetten og EU" i "*Retskildernes kamp – Forholdet mellem national offentlig ret og udefra kommende ret*" af Trine Baumbach og Peter Blume (red.), 2012, s. 51, samt Thomas Elholm: "Sanktionering af EU-retten" i "*EU-retten i Danmark*", af Birgitte Egelund Olsen og Karsten Engsig Sørensen (red.), 2018, s. 265-288. Se endvidere Helmut Satzger: *"International and European Criminal Law"*, Second Edition, 2018, s. 98 ff.

[56] Se hertil Trine Baumbach: "Strafferetten og EU" i "*Retskildernes kamp – Forholdet mellem national offentlig ret og udefra kommende ret*" af Trine Baumbach og Peter Blume (red.), 2012, s. 55, samt Baumbach: "Den retsvidenskabelige strafferetsforskning i det 21. århundrede – refleksioner", TfK 2015.515, pkt. 4.2. Se endvidere "Samarbejdet om retlige og indre anliggender. En analyse af EU-lovgivning omfattet af retsforbeholdet", marts 2015, udarbejdet af Justitsministeriet, tilgængelig på www.Justitsministeriet.dk.

jurisdiktionskompetence.[57] Andet eksempel på dansk overtagelse af EU-strafferet forelå i forbindelse med en dansk ændring i 2013 af straffelovens kapitel 24 om Seksualforbrydelser, hvor strafferammen til den nugældende § 227, stk. 2 (om at være tilskuer til en seksuel forestilling med person under 18 år) blev forhøjet til to års fængsel for at sikre overensstemmelse med et EU-direktiv.[58]

Som det ses i forhold til den materielle strafferet, synes lovgiver i Danmark at følge udviklingen i det EU-retlige samarbejde tæt og tilegne sig de strafferetlige tiltag og reguleringer, selv om Danmark qua retsforholdet ikke har haft indflydelse på den EU-retlige tilblivelse af disse retsakter. På det straffeprocessuelle område er mange vigtige instrumenter fortsat i kraft som følge af det mellemstatslige samarbejde før Lissabon-traktaten, og således er rammeafgørelsen om den europæiske arrestordre eksempelvis fortsat forpligtende for Danmark. Disse rammeafgørelser kan ikke længere udstedes, og i de tilfælde, hvor rammeafgørelser måtte blive erstattet af direktiver, vil disse på grund af det danske retsforbehold ikke være bindende for Danmark.[59]

Tredje og sidste eksempel på modifikation af udgangspunktet om, at dansk strafferet og straffeproces er nationalt reguleret, skal ses i forhold til EU-Chartret om grundlæggende rettigheder. Chartret fik traktatstatus ved Lissabon-traktatens ikrafttræden i 2009, jf. TEU art. 6, stk. 1, og bestemmelserne i Chartret er ifølge artikel 51 rettet til *"…Unionens institutioner og organer under iagttagelse af nærhedsprincippet samt til medlemsstaterne, dog kun når de gennemfører EU-retten. De respekterer derfor rettighederne, overholder principperne og fremmer anvendelsen heraf i overensstemmelse med deres respektive beføjelser."*

[57] Lov nr. 275 af 27. marts 2012, der forhøjede strafmaksimum til fængsel i 10 år og ændrede bestemmelsen i § 7, stk. 1, nr. 2, om dansk jurisdiktionskompetence, alt med henblik på at bringe dansk straffelovgivning i overensstemmelse med EP/Rdir 2011/36 om forebyggelse og bekæmpelse af menneskehandel og beskyttelse af ofrene herfor, og om erstatning af Rådets rammeafgørelse 2002/629/RIA. Se hertil Baumbach: "Strafferetten og EU" i Trine Baumbach og Peter Blume (red.): "*Retskildernes kamp – Forholdet mellem national offentlig ret og udefra kommende ret*", 2012, s. 65 ff., samt Artikel 2: *"Logning af teledata i lyset af Tele2-dommen"*, pkt. 5.

[58] Lov nr. 633 af 12. juni 2013, se hertil lovforslag nr. 141 af 6. februar 2013, pkt. 5.2.8 med henvisning til direktivet (Europa-Parlamentets og Rådets direktiv 2011/92/EU af 13. december 2011 om bekæmpelse af seksuelt misbrug og seksuel udnyttelse af børn og børnepornografi og om erstatning af Rådets rammeafgørelse 2004/68/RIA).

[59] Se Jørn Vestergaard: "EU-strafferetten og individets grundlæggende rettigheder", TfK 2016.429.

Som følge af det danske retsforbehold finder Chartret ikke umiddelbart anvendelse på de danske retlige og indre anliggender.[60] Et eksempel på, at Chartret trods retsforbeholdet alligevel får betydning for dansk straffeproces, ses af problematikken omkring logning af teledata og politiets adgang til disse data, hvor EU-domstolens afgørelse i et præjudicielt søgsmål "Tele2-sagen" om reguleringen af teleudbyderne, set i lyset af Chartrets bestemmelser, får betydning for den danske regulering.[61]

Om samspillet mellem EMRK og Chartret følger det af Chartrets artikel 52, stk. 3, at *"I det omfang dette charter indeholder rettigheder svarende til dem, der er sikret ved den europæiske konvention til beskyttelse af menneskerettigheder og grundlæggende frihedsrettigheder, har de samme betydning og omfang som i konventionen. Denne bestemmelse er ikke til hinder for, at EU-retten kan yde en mere omfattende beskyttelse."*[62]

Til spørgsmålet om, og hvilket omfang, det så er relevant at inddrage EU-retlige kilder i afhandlingens retsdogmatiske analyse, er svaret, at for reguleringen af straffeprocessuelle indgreb og politiets interageren med borgeren på internettet, vil EU-retten som udgangspunkt være af begrænset relevans, bortset fra området for indgreb i meddelelseshemmeligheden, hvor EU med dommen i Tele2-sagen har fastlagt nogle ret håndfaste grænser og kriterier for logning af teledata og politiets adgang til disse data. I relation til den danske 'hacking'-bestemmelse i straffelovens § 263 inddrages Cybercrimedirektivet med et retspolitisk sigte, som inspiration til en snævrere kriminalisering.

I det følgende skal gøres et par bemærkninger om EU-retskilderne, navnlig om EU-samarbejdets tiltag i forhold til cybercrime, jf. Cybercrimedirektivet, samt Europol-samarbejdet.

2.2.1. EU-retskilder

Retskilderne i EU-samarbejdet udgøres af traktater, direktiver, domspraksis og afgørelser foruden forskellige henstillinger og udtalelser af ikke-bindende karakter. Dette afsnit vil angå de retsakter, der har betydning for samarbejdet om strafferet og politi, særligt de retsakter der har fokus på bekæmpelse af IT-kriminalitet.

Det fremgår af TEUF artikel 83, at Europa-Parlamentet og Rådet ved direktiv kan fastsætte minimumsregler for, hvad der skal anses for strafbare handlinger, samt straffene herfor på områder med kriminalitet af særlig grov karakter, der har en

[60] Jf. Jonas Christoffersen m.fl.: *"EU's Charter om Grundlæggende rettigheder med kommentarer"*, 2018, s. 71 ff., om det danske retsforbehold.
[61] Nærmere herom i Artikel 2: "*Logning af teledata i lyset af Tele2-dommen.*"
[62] Se hertil, bl.a. Jonas Christoffersen m.fl.: *"EU's Charter om Grundlæggende rettigheder med kommentarer"*, 2018, s. 75 ff.

grænseoverskridende dimension som følge af overtrædelsernes karakter eller konsekvenser eller af et særligt behov for at bekæmpe dem på fælles grundlag.[63] Følgende kriminalitetsområder er nævnt: terrorisme, menneskehandel og seksuel udnyttelse af kvinder og børn, ulovlig narkotikahandel, ulovlig våbenhandel hvidvaskning af penge, korruption, forfalskning af betalingsmidler, *edb-kriminalitet* og organiseret kriminalitet (min kursivering). Derudover følger af artikel 83, stk. 2, at minimumsregler kan fastsættes for andre områder, hvis det viser sig *absolut nødvendig* for at sikre gennemførelsen af en EU-politik (min kursivering).

I medfør af TEUF artikel 83, stk. 1 har Europa-Parlamentet og Rådet den 12. august 2013 vedtaget et direktiv (2013/40/EU) om angreb på informationssystemer og om erstatning af Rådets rammeafgørelse 2005/222/RIA (Cybercrimedirektivet). Direktivet gælder ikke for Danmark, men da direktivet i vidt omfang bygger på rammeafgørelse 2005/222/RIA og Europarådets Konvention om IT-kriminalitet af 23. november 2001, som Danmark har tiltrådt og implementeret på mellemstatsligt grundlag, er der i vidt omfang allerede overensstemmelse mellem Cybercrimedirektivet og dansk ret.[64] Direktivet indeholder ikke bestemmelser om gensidig anerkendelse, men alene nye elementer, som vil kunne tilvælges og gennemføres i dansk ret.

Cybercrimedirektivet var en del af den tilvalgsordning, der blev afvist ved folkeafstemningen i december 2015.[65] Det er endnu uvist, om man fra lovgivers side vil 'genoptage' direktivet til den normale procedure, hvor det gennemgås, og der sikres overensstemmelse med dansk ret.

Europol-samarbejdet er med hjemmel i TEUF artikel 88 blevet et overstatsligt samarbejde, som nu er reguleret ved Europol-forordningen, der trådte i kraft den 1. maj 2017.[66] Efter afvisningen af tilvalgsordningen, indgik Danmark en samarbejdsaftale om Europol på mellemstatsligt grundlag. Europols målsætning efter forordningens artikel 3, stk. 1, er at "støtte og styrke medlemsstaternes kompetente myndigheders

[63] Jf. Artikel 2: *"Logning af teledata i lyset af Tele2-dommen"*, pkt. 3.1.2.

[64] Rammeafgørelsen 2005/222/RIA og Europarådets Konvention af 23. november 2001 om IT-kriminalitet blev begge gennemført i dansk ret ved lov nr. 352 af 19. maj 2004. Se om dansk rets overensstemmelse hermed, lovforslag nr. 55 af 5. november 2003, pkt. 7 og 8. Se endvidere Justitsministeriets notat om tilvalg af Cybercrimedirektivet, offentliggjort den 17. marts 2015 på http://justitsministeriet.dk/nyt-og-presse/pressemeddelelser/2015/aftale-om-en-tilvalgsordning

[65] Lovforslag 29, "Forslag til lov om omdannelse af retsforbeholdet til en tilvalgsordning", fremsat den 8. oktober 2015.

[66] Europa-Parlamentets og Rådets forordning (EU) 2016/794 af 11. maj 2016 om Den Europæiske Unions Agentur for Retshåndhævelsessamarbejde (Europol) og om erstatning og ophævelse af Rådets afgørelse 2009/371/RIA, 2009/934/RIA, 2009/935/RIA, 2009/936/RIA og 2009/968/RIA.

indsats for og deres indbyrdes samarbejde om at forebygge og bekæmpe grov kriminalitet, der berører to eller flere medlemsstater, samt terrorisme og former for kriminalitet, der berører en fælles interesse, som er omfattet af en EU-politik, jf. listen i bilag I."[67] Fra denne liste kan her fremhæves af relevans for efterforskning på internettet: terrorisme, organiseret kriminalitet, narkotikahandel, bedrageri, efterligninger og fremstilling af piratudgaver af produkter, IT-kriminalitet, seksuelt misbrug og seksuel udnyttelse, herunder materiale, der viser misbrug af børn, og hvervning af børn til seksuelle formål.[68]

Europol udgiver årlige rapporter om vurderingen af truslen fra internetkriminalitet – The Internet Organised Crime Threat Assessment (IOCTA).[69]

I regi af Europa-Parlamentet blev i 2017 udarbejdet en undersøgelse af udvalgte landes regulering af politiets 'hacking' som led i en efterforskning: "Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of practices", Study for the LIBE Committee (European Parliament's Committee on Civil, Liberties, Justice and Home Affairs.[70] Rapporten giver et overblik over de overvejelser, der indgår ved regulering af kryptering og 'hacking'-metoder, og indeholder en række anbefalinger til 'best practice' for national regulering. Rapporten indgår i en perspektivering på en mulig dansk 'hacking'-bestemmelse, jf. Del 3, Kapitel 3, afsnit 4.

For politiets indsamling af data gælder retshåndhævelsesdirektivet,[71] for selvom Danmark ikke er bundet af direktivet som følge af retsforbeholdet, har man tilsluttet sig direktivet på mellemstatsligt grundlag og implementeret direktivet ved lov.[72]

---

[67] Omfattet af Europols målsætning er også en række relaterede strafbare handlinger til disse kriminalitetsformer, jf. forordningens artikel 3, stk. 2.

[68] Jf. Artikel 2: *"Logning af teledata i lyset af Tele2-dommen"*, pkt. 3.1.2.

[69] Tilgængelig på Europols hjemmeside: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment

[70] Tilgængelig på Europaparlamentets hjemmeside: http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf

[71] Europa-Parlamentets og Rådets direktiv (EU) 2016/680 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med kompetente myndigheders behandling af personoplysninger med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner og om fri udveksling af sådanne oplysninger og om ophævelse af Rådets rammeafgørelse 2008/977/RIA.

[72] Lov nr. 410 af 27. april 2017 om Retshåndhævende myndigheders behandling af personoplysninger. Peter Blume har forholdt sig til politipersondatadirektivets krav om formålsbestemthedsprincippet og undtagelserne hertil i U 2016B.338 "Formålsbestemthed."

Disse regler udgør en særlig regulering for de retshåndhævende myndigheder, hvilket udelukker de almindelige databeskyttelsesregler på dette område.[73]

EU-domstolens kompetence spænder vidt fra traktatbrudssøgsmål, annullationssøgsmål og passivitetssøgsmål mv. I denne sammenhæng skal blot fremhæves muligheden for præjudicielle søgsmål, hvor nationale domstole som led i afgørelsen af en konkret retssag i medfør af TEUF art. 267 kan forelægge et spørgsmål for EU-Domstolen om fortolkningen af traktaterne og om gyldigheden og fortolkningen af retsakter udstedt af Unionens institutioner, organer, kontorer eller agenturer.[74] EU-Domstolen har i sager med præjudicielle søgsmål kompetence til at udtale sig om fortolkningen, anvendelsen og gyldigheden af en EU-retsakt, mens det ikke tilkommer Domstolen at tage stilling til fortolkningen af national ret, men EU-Domstolens fortolkning af EU-retsakten kan ses som en vejledning til den nationale ret.[75] Præjudicielle søgsmål var baggrunden for sagerne vedrørende logning (Digital Rights og Tele2-sagerne), som indgår i Artikel 2: "*Logning af teledata i lyset af Tele2-dommen*" og Artikel 3: "*Retsplejelovens regulering af politiets adgang til teledata*."

Der er således ikke i EU-regi etableret en egentlig klageadgang for den enkelte borger for – efter udtømmelse af nationale retsmidler – at få EU-domstolens stillingtagen til Chartrets rettigheder, som det ses i forhold til EMRK.[76]

2.2.2. EU-fortolkningsprincipper

For EU-retten gælder en række fortolkningsprincipper, der er særlige for dette samarbejde, og som Danmark er forpligtet af. Af relevans for forholdet mellem dansk ret og EU-ret, gælder først og fremmest det EU-retlige legalitetsprincip, hvorefter hver institution handler inden for de beføjelser, den er tillagt, jf. princippet om kompetencetildeling i TEU art. 5. Princippet markerer dels kompetencefordelingen mellem medlemsstaterne og Unionen, dels det "klassiske" legalitetsprincip, at Unionens lovgivning og retsakter med virkning for medlemsstaterne og deres myndigheder samt unionsborgerne, skal have hjemmel i traktaterne.[77]

---

[73] Lovforslag nr. 168 af 28. marts 2017, pkt. 1.1. (til lov nr. 410 af 27.april 2017).
[74] Jf. Christina D. Tvarnø og Ruth Nielsen: "*Retskilder og retsteorier*", 2017, s. 150 ff.
[75] Jf. Jonas Christoffersen m.fl.: *"EU's Charter om Grundlæggende rettigheder med kommentarer"*, 2018, s. 63 f. Det er således ikke helt præcist formuleret at beskrive EU-Domstolen som konfliktløsende, jf. Artikel 2: *"Logning af teledata i lyset af Tele2-dommen"*, pkt. 3.
[76] Dog kan annullationssøgsmål anlægges efter TEUF artikel 263 af "ikke-privilegerede sagsøgere", se herom Karsten Engsig Sørensen og Jens Hartig Danielsen: *"EU-retten"*, 2019, s. 227 f.
[77] Jf. Karsten Engsig Sørensen og Jens Hartig Danielsen: *"EU-retten"*, 2019, s. 125 ff.

EU-domstolen har fastslået, at medlemsstaterne har pligt til at fortolke national ret i overensstemmelse med de EU-retlige regler, såkaldt "EU-konform-fortolkning",[78] ligesom EU-domstolen har fastslået, at EU-retten har forrang frem for national ret.[79] Domstolen har desuden i *CILFIT-sagen* fremhævet, at de EU-retlige bestemmelser er affattet på flere forskellige sprog, og at alle sproglige versioner er autentiske, ligesom det i sagen blev fastslået, at de enkelte EU-regler skal vurderes i deres rette sammenhæng og fortolkes i lyset af EU-rettens bestemmelser som helhed, den bagvedliggende målsætning og EU-rettens udviklingstrin på tidspunktet for de pågældende bestemmelsers anvendelse.[80]

2.3. Europarådets Cybercrimekonvention

Europarådet[81] har udarbejdet Konvention af 23. november 2001 om cybercrime ("Budapest-konventionen", ETS no. 185), og Konventionen er nu ratificeret af 52 lande, herunder USA, Canada, Japan, Sydafrika, Australien og Israel.[82]

Formålet med Konventionen er at styrke efterforskningen og strafforfølgningen af IT-kriminalitet. Konventionen indeholder en række definitioner af bl.a. "edb-system" mv. for at sikre en fælles forståelse af begreberne.[83] Mere konkret indeholder Konventionen en række forpligtelser for de deltagende stater særligt med hensyn til kriminalisering af forskellige former for IT-kriminalitet og med hensyn til efterforskning og internationalt samarbejde på området.[84] I tilknytning til Konventionen har Euro-

[78] Se bl.a. Karsten Engsig Sørensen og Jens Hartig Danielsen: *"EU-retten"*, 2019, s. 161 ff*.,* og Christina D. Tvarnø og Ruth Nielsen: "*Retskilder og retsteorier*", 2017, s. 115 f. og 205 ff.

[79] Jf. Jonas Christoffersen m.fl.: *"EU's Charter om Grundlæggende rettigheder med kommentarer"*, 2018, s. 51, med henvisning til EU-domstolens afgørelse i *Costa mod ENEL*-sagen, Sag 6/64, og i samme retning, Karsten Engsig Sørensen og Jens Hartig Danielsen: *"EU-retten"*, 2019, s. 185 ff. Her udelades diskussionen om EU-rettens forrang frem for Grundloven, jf. U 1998.800 H, og Karsten Engsig Sørensen og Jens Hartig Danielsen: *"EU-retten"*, 2019, s. 187.

[80] *CILFIT*-sagen 283/81, præmis 18-20, jf. hertil Karsten Engsig Sørensen og Jens Hartig Danielsen: *"EU-retten"*, 2019, s. 116 f.

[81] Europarådet er et mellemstatsligt samarbejde af 47 lande, hvoraf indgår alle EU-lande.

[82] http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

[83] Om Konventionen, se Inger Marie Sunde: "Cybercrime Law" i *"Digital Forensics"* af André Årnes (ed.), 2018, s. 51 ff.

[84] Lovforslag nr. 55 af 5. november 2003, pkt. 7, til lov nr. 352 af 19. maj 2004 hvor Konventionen blev gennemført i straffeloven, retsplejeloven, markedsføringsloven og ophavsretsloven. Enkelte af Konventionens bestemmelser blev gennemført ved

parådet udarbejdet en "*Explanatory report*", der dog ikke udgør en bindende fortolkning til Konventionen, jf. rapportens indledende bemærkning, og derudover udstedes ligeledes en række *"Guidance Notes"* til Konventionen.[85]

Gennemførelsen i dansk ret skete i 2004 ved, at der indholdsmæssigt sikredes, at den danske regulering var i overensstemmelse med Konventionen,[86] hvilket bl.a. medførte, at straffelovens § 293, stk. 2 om rådighedshindring blev præciseret til også at omfatte rådighedshindring ad elektronisk vej. Derudover blev forskellige uretmæssige aktiviteter vedrørende adgangsmidler kriminaliseret i straffelovens § 301, § 301 a og § 263 a og dokumentfalskbestemmelsen i § 171 blev udvidet til også at omfatte elektroniske dokumenter. Straffeprocessuelt medførte Konventionen, at der i retsplejeloven blev indsat hjemmel til hastesikring af indholdsdata og trafikdata, jf. retsplejelovens § 786 a.

Her må kort nævnes, at Europarådet i 2003 vedtog en supplerende protokol til Konventionen ("Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems" (ETS No. 189)). Ligeledes i Europarådet blev i 2007 vedtaget "Convention on Protection of Children against Sexual Exploitation and Sexual Abuse"(ETS No. 201), som indeholder en række krav til kriminalisering af seksuelle forbrydelser mod børn mv.

2.4. Den Europæiske Menneskerettigheds Konvention (EMRK)

Ligeledes i regi af Europarådet er vedtaget Den Europæiske Menneskerettighedskonvention, der trådte i kraft i 1953. EMRK blev inkorporeret i dansk ret ved lov nr. 285 af 29. april 1992.[87]

Konventionen indeholder et udførligt rettighedskatalog, hvor det for flere af rettighederne er foreskrevet, at indgrebet skal være bestemt ved lov, og at indgrebet alene må ske, hvis det er nødvendigt (proportionalitetsprincip) for at varetage nær-

---

lov nr. 228 af 2. april 2003 om ændring af straffeloven, adoptionsloven og retsplejeloven (Børnepornografi, seksuel udnyttelse af børn, salg af børn og gennemførelse af straffesager om seksuelt misbrug af børn mv.)

[85] Jf. Artikel 1: *"'Hacking' og det digitale privatliv*, pkt. 1.

[86] Lovforslag nr. 55 af 5. november 2003, pkt. 7.

[87] Se hertil Bet. 1220/1991 om Den Europæiske Menneskerettighedskonvention og dansk ret samt lovforslag nr. 230 af 19. februar 1992 til inkorporeringsloven. Om betydningen af inkorporering af internationale konventioner, se bl.a. Pernille Boye Koch: "Lovgivers rolle som fortolker af internationale retskilder – på hvilken måde gælder menneskerettighederne i Danmark?", Tidsskrift for Rettsvitenskap, vol. 132, 1/2019, s. 3-50.

mere bestemte konkrete hensyn, således i relation til indgreb i privatlivet, religionsfriheden, ytringsfriheden og forsamlingsfriheden, jf. artikel 8-11. Enkelte af Konventionens rettigheder er absolutte, således at der ikke kan gøres undtagelse, eksempelvis artikel 3 om forbud mod tortur, umenneskelig eller nedværdigende behandling eller straf, artikel 7 om princippet om ingen straf uden retsregel, samt artikel 12 om retten til at indgå ægteskab.

Særligt for denne afhandlings analyse af straffelovens 'hacking'-bestemmelse er EMRK art. 7 om det strafferetlige legalitetsprincip relevant. For de straffeprocessuelle tvangsindgreb er artikel 8 relevant, når det gælder indgreb i privatliv og familieliv, hjem og korrespondance. I relation til agentvirksomhed og infiltration er den menneskeretlige beskyttelse mod politiets provokation udviklet gennem EMD-praksis i relation til artikel 6 om 'fair trial', som også er af generel betydning for den straffeprocessuelle regulering. EMD's fortolkning af disse rettigheder får i disse år øget betydning for den danske nationale regulering af politiets efterforskning, i forhold til hvilke af politiets metoder, der indebærer et indgreb i borgernes rettigheder, og som derfor forudsætter en retlig regulering, ligesom Domstolen i visse tilfælde giver ret præcise anvisninger til indholdet af en sådan regulering, jf. denne afhandlings tema om det straffeprocessuelle legalitetsprincip.

Klagesystemet i EMRK er etableret som en direkte klageadgang for enkeltpersoner, grupper af personer og non-governmental organisations (NGO'er), jf. EMRK art. 34, dog kræves, at nationale retsmidler er udtømt, jf. art. 35. Derudover er der klageadgang for stater over andre staters brud på Konventionen, jf. artikel 33. Det følger af art. 46, stk. 1, at medlemslandene er forpligtet til at efterleve Den Europæiske Menneskerettighedsdomstols (EMD) afgørelse i enhver sag, landene er parter i.

En reformproces af EMD er igangsat, bl.a. for at sikre mere effektiv national implementering af EMRK og EMD's afgørelser, ud fra tanken om, at beskyttelsen af menneskerettighederne beror på "shared responsibility" mellem EMD og nationalstaterne, jf. subsidaritetsprincippet nedenfor, ligesom fokus bl.a. er på en mere effektiv sagsbehandling ved EMD og at nedbringe en ophobet sagsmængde.[88]

Som retskilder betragtes først og fremmest konventionsteksten, foruden domme afsagt af EMD, foruden domstolens afgørelse om realitetsbehandling af klager ("admissibility"). Domstolens afgørelser vil have præjudikatsværdi ved fortolkning af ret-

[88] Se hertil "Copenhagen Declaration" af 13. april 2018.
LINK: https://www.echr.coe.int/Documents/Copenhagen_Declaration_ENG.pdf

tigheder og forpligtelser i EMRK, således at andre stater, der ikke indretter sin retstilstand i overensstemmelse hermed, må forvente at kunne blive dømt for krænkelse af Konventionen.[89]

I regi af EMD er udarbejdet forskellige Factsheets og Guidelines over Domstolens praksis om EMRK, eksempelvis "*Guide on Article 8 of the European Convention on Human Rights – Right to respect for private and family life, home and correspondence*", opdateret den 30. april 2019, og "*Guide on Article 6 of the European Convention on Human Rights - Right to a fair trial (criminal limb)"*, opdateret den 30. april 2019.[90] Disse guidelines, som dog ikke er bindende for EMD, giver en oversigt og en systematik til forståelsen af Domstolens righoldige retspraksis på disse områder.

Fastlæggelse af det nærmere indhold af EMRK's rettigheder og fortolkning af de enkelte bestemmelser i Konventionen kan forekomme i to sammenhænge: Den Europæiske Menneskerettighedsdomstol, som først og fremmest – og som ovenfor nævnt autoritativt – fastlægger og fortolker rettighedernes indhold, og de enkelte medlemslande, som generelt må følge og indarbejde den retstilstand der fastlægges af EMD.

Dog følger det af 'subsidaritetsprincippet' i EMRK artikel 13 og 35, stk. 1, at beskyttelsen af borgerens menneskerettigheder først og fremmest sker ved, at nationale retsinstanser anvender og fortolker rettighederne i konkrete sager, og at retsbeskyttelsen ved EMD er subsidiær, da klageadgang til Domstolen først er aktuel, når nationale retsmidler er udtømt.[91]

I det følgende behandles først fortolkningsprincipperne for EMD, dernæst de særlige forhold der gør sig gældende for fortolkningen ved de danske domstole.

2.4.1. Den Europæiske Menneskerettighedsdomstols fortolkningsprincipper

EMD fortolker Konventionen med udgangspunkt i folkerettens regler om traktatfortolkning, hvoraf følger, at en traktat i første række skal fortolkes i overensstemmelse med den enkelte bestemmelses ordlyd, dennes kontekst og formålet med traktaten

[89] Baumbach: "*Strafferet og menneskeret*", 2014, s. 23 f., og Jens Elo Rytter: *"Individets grundlæggende rettigheder"*, 2019, s. 81.
[90] Disse case-law guides kan findes på EMD's hjemmeside: www.echr.coe.int (Case-law – Case-law analysis – Case-law guides).
[91] jf. Artikel 5: *"Politiets infiltration på digitale platforme – set i et menneskeretligt perspektiv"*, pkt. 4.3.

som helhed.[92] I relation til ordlydsfortolkningen må nævnes, at de officielle og juridisk bindende tekster er engelsk og fransk. Forarbejder til Konventionens bestemmelser spiller kun en meget begrænset rolle, derimod inddrager EMD i vidt omgang de enkelte rettigheders 'formål' og 'mening' for at sikre en reel og effektiv retsbeskyttelse for individet.[93] EMD fortolker de enkelte rettigheder i lyset af Konventionen som helhed for at sikre indre sammenhæng og undgå indbyrdes modsigelser.[94]

Rettighederne i EMRK er hovedsageligt formuleret negativt, forstået som grænser for staternes indgreb, men EMD har i flere sammenhænge fastsat positive forpligtelser for staterne til at sikre rettigheders beskyttelse.[95]

EMD's fortolkningsstil betegnes som 'dynamisk', idet rettighedsbeskyttelsen videreudvikles i takt med rets- og samfundsudviklingen i medlemslandene.[96] Af EMD formuleret: *"The Convention is a living instrument which must be interpreted in the light of present-day conditions."*[97] Hvorvidt EMD's fortolkningsstil er for dynamisk eller politisk har været genstand for debat i hjemlige juridiske kredse.[98] Det sker, at EMD

---

[92] Wiener-Konventionen af 23. maj 1969 om traktatretten, navnlig artikel 31, stk. 1, se hertil Rytter: *"Individets grundlæggende rettigheder"*, 2019, s. 83, Kjølbro: *"Den Europæiske Menneskerettighedskonvention for praktikere",* 2017*,* s. 21, og Frederik Harhoff m.fl.: *"Folkeret"*, 2017, s. 128 ff.

[93] Rytter: *"Individets grundlæggende rettigheder"*, 2019, s. 81 og 85, og Kjølbro: *"Den Europæiske Menneskerettighedskonvention for praktikere"*, 2017, s. 24 f.

[94] Rytter: *"Individets grundlæggende rettigheder"*, 2019, s. 83, samt Kjølbro: *"Den Europæiske Menneskerettighedskonvention for praktikere"*, 2017, s. 22 f., med henvisning til bl.a. *Stec og andre mod Storbritannien*, afgørelse om realitetsbehandling af 6. juli 2005, pkt. 48.

[95] Rytter: *"Individets grundlæggende rettigheder"*, 2019, s. 67 ff., og Kjølbro: *"Den Europæiske Menneskerettighedskonvention for praktikere"*, 2017, s. 27 f.

[96] Rytter: *"Individets grundlæggende rettigheder"*, 2019, s. 81, Kjølbro: *"Den Europæiske Menneskerettighedskonvention for praktikere"*, 2017, s. 25 f., og Rainey, B., E. Wicks and C. Ovey: "*The European Convention on Human Rights*", 7th edition, 2017, s. 76 ff.

[97] Rytter: *"Individets grundlæggende rettigheder"*, 2019, s. 86, med henvisning til *Tyrer mod Storbritannien*, dom af 25. april 1978, pkt. 31, og *Mazurek mod Frankrig*, dom af 1. februar 2000, pkt. 49.

[98] Se bl.a. Juristen, 2017, nr. 3, "Temanummer Menneskerettighedsdomstolens retsanvendelse." Desuden Børge Dahl: "Dynamiske domstole, retssikkerhed og demokrati: Skal menneskerettigheder udvikles af politikere eller dommere?" og Jon Fridrik Kjølbro: "Den Europæiske Menneskerettighedsdomstol: Praktiske udfordringer, juridiske udfordringer og et spørgsmål om legitimitet", begge i Juristen 2017, nr. 5.

ved denne dynamiske fortolkning af rettighedernes indhold undersøger, hvorvidt der foreligger fælles standarder i medlemsstaternes nationale retssystemer, som kan danne grundlag for en dynamisk udbygning af EMRK-beskyttelsen.[99] Et eksempel herpå er EMD' dom i *Veselov og andre mod Rusland*, som indeholder en komparativ gennemgang af 22 af Europarådets medlemsstaters regulering af agentvirksomhed, jf. EMRK artikel 6, stk. 1.[100]

Særligt i relation til frihedsrettighederne i EMRK artikel 8-11, følger det af bestemmelsernes stk. 2, at indgreb i disse rettigheder kun kan ske, hvis indgrebet sker i overensstemmelse med loven og er nødvendigt i et demokratisk samfund af hensyn til en af de nærmere opregnede formål i bestemmelserne. Heri ligger først og fremmest et legalitetskrav, og dernæst et proportionalitetsprincip, i tilknytning til hvilket EMD har udviklet et princip om "margin of appreciation". Herved forstås, at der overlades en vis skønsmargin til de enkelte medlemslande til at foretage denne afvejning, hvilket bevirker, at EMD udviser en vis tilbageholdenhed.[101]

2.4.2. Danske fortolkningsprincipper i forhold til EMRK

Det følger af EMRK artikel 1, at staterne skal sikre Konventionens rettigheder for enhver person inden for statens jurisdiktion, men Konventionen tager ikke stilling til, *hvordan* rettighederne skal sikres nationalt og påberåber sig således ikke som EU-retten en direkte virkning.[102] I kraft af 1992-inkorporeringsloven må EMRK som udgangspunkt have forrang for eventuel modstrid med almindelig lovgivning, hvilket indebærer, at en dansk lovbestemmelse, der er uforenelig med EMRK, som denne til enhver tid fortolkes af EMD, må tilsidesættes af danske domstole, medmindre de danske lovgivere udtrykkeligt har ønsket at fravige EMRK.[103]

Endvidere Eva Smith: "Højesteret og Den Europæiske Menneskerettighedskonvention" i Juristen 2018, nr. 2, s. 73, foruden Jens Vedsted-Hansen: "Danske udfordringer i det europæiske menneskerettighedssystem", Juristen 2017, nr. 6, s. 236.

[99] Rytter: *"Individets grundlæggende rettigheder"*, 2019, s. 87.

[100] *Veselov og andre mod Rusland*, dom af 2. oktober 2012, pkt. 50-63, jf. hertil Artikel 6: *"Politiagenter i et menneskeretligt perspektiv"*, pkt. 4.4.

[101] Rytter: *"Individets grundlæggende rettigheder"*, 2019, s. 112 ff., Kjølbro: *"Den Europæiske Menneskerettighedskonvention for praktikere"*, 2017, s. 26 f. og 768 ff., samt Rainey, B., E. Wicks and C. Ovey: "*The European Convention on Human Rights*", 7th edition, 2017, s. 81 ff. og 360 ff. Princippet om 'margin of appreciation' indgår i Artikel 2: *"Logning af teledata i lyset af Tele2-dommen"*, pkt. 3.2, og Artikel 5: *"Politiets infiltration på digitale platforme – set i et menneskeretligt perspektiv"*, pkt. 4.3.

[102] Rytter: *"Individets grundlæggende rettigheder"*, 2019, s. 54.

[103] Rytter: *"Individets grundlæggende rettigheder"*, 2019, s. 56 f. Se hertil Bet. 1220/1991, s. 196, samt lovforslag nr. 230 af 19. februar 1992, pkt. 4.3.1. og pkt. 5 til inkorporeringsloven (lov nr. 285 af 29. april 1992). Om lovgivers ansvar for løbende at sikre dansk rets overensstemmelse med internationale konventioner, se

2.5. Øvrige retskilder

I relation til de retspluralistiske aspekter, som indgår som en vigtig kontekst for afhandlingens temaer, vil i afhandlingens analyser på relevante steder indgå en beskrivelse af nogle af de gængse digitale platforme og sociale medier og de brugervilkår, man giver samtykke til, ved oprettelse af brugerprofiler, ligesom databeskyttelsesreguleringen i mindre grad vil indgå.

3. Afhandlingens form og forløb

I dette afsnit redegøres først for baggrunden for, at afhandlingen er udarbejdet artikelbaseret i stedet for som en monografi. Dernæst redegøres for afhandlingens forløb, nærmere forstået hvordan det kunne sikres undervejs at have en opdateret viden om de politioperative aspekter og muligheder i relation til digital efterforskning.

3.1. Begrundelse for artikelbaseret

Som det fremgår ovenfor, indgår de seks artikler som elementer i en samlet analyse af politiets hemmelige efterforskning på internettet med udgangspunkt i de konkrete forskningsspørgsmål. Afhandlingen kunne derfor være udarbejdet som en monografi.

Beslutningen om at udarbejde afhandlingen artikelbaseret beror på den hastige teknologiske udvikling både i forhold til mulighederne for IT-kriminalitet og i forhold til politiets metoder til efterforskning af denne kriminalitet, hvor det af hensyn til forskningens aktualitet og relevans kunne være en fordel at publicere resultaterne undervejs. Dette ville tillige give mulighed for at drøfte de forskningsmæssige resultater med relevante repræsentanter fra politi, anklagemyndighed og advokatbranchen, ligesom der kan være en helt aktuel, lovgivningsmæssig, politisk kontekst, som det kunne være relevant med artiklerne at bidrage til. På baggrund af feedback og eventuelle lovgivningsmæssige tiltag og ny retspraksis, ville det være muligt at lave en opfølgende analyse og videreudvikle begrebssættet i afhandlingens ramme, der således ved indlevering til bedømmelse kunne fremstå helt opdateret og relevant.

Beslutningen om at udarbejde afhandlingen artikelbaseret er kun blevet bekræftet undervejs, hvor afhandlingens temaer har vist sig i høj grad at være aktuelle. Således kunne det på baggrund af Artikel 2: "*Logning af teledata i lyset af Tele2-dommen*" og Artikel 3:"*Retsplejelovens regulering af politiets adgang til teledata*" konkluderes,

---

Pernille Boye Koch: "Lovgivers rolle som fortolker af internationale retskilder – på hvilken måde gælder menneskerettighederne i Danmark?", Tidsskrift for Rettsvitenskap, vol. 132, 1/2019, s. 3-50.

at EU-domstolens afgørelse i Tele2-sagen ville medføre, at retsplejelovens regulering om indgreb i meddelelseshemmeligheden mv. snarest må forventet ændret for at sikre overensstemmelse med Tele2-dommen, uden at dette dog endnu er sket. Der verserer pt. et sagsanlæg fra Foreningen mod Ulovlig Logning mod Justitsministeriet. I juni 2019 kom det desuden frem, at en alvorlig fejl i Rigspolitiets IT-system har påvirket de teledata, der modtages fra teleselskaberne, således at der i visse tilfælde har manglet "linjer" (opkald, masteposition mv.) i det materiale, der har indgået i straffesagerne. Rigsadvokaten har meddelt, at 10.000 sager nu skal manuelt gennemgås for at vurdere, om sagerne har været berørt af denne systemfejl.

Efter at have indleveret Artikel 1: "*'Hacking' og det digitale privatliv*" til bedømmelse hos tidsskriftet Juristen, blev der fremsat et lovforslag om ændring af straffelovens 'hacking'-bestemmelse, hvilket gav anledning til på baggrund af artiklen at udarbejde et høringssvar til lovforslaget[104] og affatte en kronik om 'hacking'-bestemmelsen, der blev trykt i Information.[105]

I foråret 2019, mens arbejdet med afhandlingens temaer om infiltration og agentvirksomhed var i gang, blev fremsat et lovforslag (L 197) som indebar en udvidet adgang til at iværksætte agentvirksomhed i fire former for kriminalitet, hvor "overtrædelsen begås ved brug af internettet". Lovforslaget bortfaldt dog som følge af folketingsvalget i juni 2019, men kan eventuelt forventes genfremsat. Disse mulige nye tiltag indgik i de strategiske overvejelser om temaet for Artikel 6, hvilket der redegøres nærmere for i Del 3, Kapitel 4.

Alt i alt har udviklingen over de seneste tre år bekræftet områdets dynamiske karakter, hvilket støtter begrundelsen for at udarbejde afhandlingen artikelbaseret.[106]

3.2. Opdateret viden om det politioperative aspekt

Når formålet med denne afhandling er at afdække den retlige regulering for politiets hemmelige efterforskning på internettet, kræver det en grundlæggende og opdateret indsigt i, hvad politiet rent faktisk foretager sig i den digitale efterforskning af konkrete straffesager. Der er ikke offentligt tilgængelige retskilder om dette rent operative og politifaglige aspekt, men en vis indsigt i de konkrete metoder, der anvendes, følger af forfatterens tidligere ansættelse i anklagemyndigheden, jf. nedenfor.

---

[104] Høringssvar af 22. august 2018, tilgængelig på: https://www.ft.dk/samling/20181/lovforslag/L20/bilag/10/1985947.pdf

[105] "Kan det virkelig være rigtigt, at 'facerape' skal være strafbart?", kronik i Information den 1. november 2018, tilgængelig på: https://www.information.dk/debat/2018/10/kan-virkelig-vaere-rigtigt-facerape-vaere-strafbart?lst_cntrb.

[106] Kronologisk rækkefølge for artiklernes udarbejdelse: Artikel 2, 3, 1, 4, 5 og 6.

For at skrive meningsfuldt om de retlige rammer for politiets hemmelige efterforskning på internettet er det imidlertid ikke tilstrækkeligt at have et øjebliksbillede af de digitale efterforskningsmetoder, politiet anvender. Den hastige teknologiske udvikling på området for efterforskning af IT-kriminalitet gør, at man løbende må orientere sig i de nye tiltag, politiet udvikler inden for dette område.

Dette ph.d.-projekt har været forankret i forskningscenteret, Center for Cyberkriminalitet og Cybersikkerhed, som i 2017 var vært for Nordisk Cybercrimeseminar med henblik på at idéudveksle med nordiske forskere inden for cybercrime, ligesom der også til seminaret var inviteret aktører fra den praktiske verden, såsom repræsentanter fra Rigspolitiet og Rigsadvokaten. Ved seminaret blev etableret et Nordisk Cybercrime-netværk, både med forskere og myndighedsudøvere på området. Netværket, som havde lejlighed til igen at mødes i København i 2018, har været til stor nytte i forhold til diskussion af denne afhandlings temaer. Ligeledes ved de årlige Nordiske Strafferetsworkshops – i Stavern, Norge i 2017, og i Lund, Sverige i 2018 – har de nordiske strafferetskolleger bidraget med konstruktiv feedback til afhandlingens temaer og metode. Desuden gav et forskningsophold i april og juli 2018 ved den norske Politihøgskole i Oslo mulighed for at drøfte afhandlingens temaer med norske strafferetsforskere, kriminologer og politifaglige kolleger.

I 2017 blev etableret en kontaktgruppe mellem strafferetsgruppen ved Juridisk Institut/AAU og Nordjyllands Politi til vidensdeling og refleksion om ny kriminalitet og nye efterforskningsmæssige metoder. Arbejdet i kontaktgruppen giver også et væsentligt udbytte i forhold til udvikling af nye forskningsmæssige projekter på det strafferetlige og straffeprocessuelle område. Flere af afhandlingens tekniske aspekter har været drøftet med bl.a. lektor Jens Myrup Pedersen, Institut for Elektroniske Systemer, Aalborg Universitet, og Sonny Olesen fra Nationalt Cybercrimecenter (NC3) under Rigspolitiet.

Som det ses, har det været prioriteret undervejs i afhandlingens forløb på flere måder at sikre opdateret viden om politiets operative arbejde og de metoder, der udvikles til efterforskning på internettet. Den tekniske og juridisk forskningsmæssig sparring undervejs har uden tvivl øget kvaliteten i afhandlingens analyser. For at sikre en afbalanceret sparring er tillige gjort uformelt brug af en række forsvarsadvokater med interesse for IT-kriminalitet og digital efterforskning, ligesom der undervejs har været kontakt til flere privacy-aktører, blandt andre Jesper Lund fra IT-politisk forening.

4. Forfatterens forskningsmæssige integritet

På dette sted i fremstillingen er det relevant at gøre en bemærkning af personlig karakter i relation til min forskningsmæssige integritet. Jeg har fra 2006 til maj 2019 været ansat som anklager på Justitsministeriets område, senest hos Nordjyllands Politi, hvor jeg var beskæftiget med IT-kriminalitet i form af straffesager om bedrageri,

databedrageri, 'hacking' og fredskrænkelser på internettet, samt efterforskningen af disse forbrydelser. Siden december 2015 har jeg haft orlov fra ansættelsen, først til en stilling som videnskabelig assistent og siden 1. august 2016 til et ph.d.-stipendiat ved Center for Cyberkriminalitet og Cybersikkerhed, Juridisk Institut, Aalborg Universitet. Jeg ansøgte om afsked fra anklagemyndigheden med virkning fra udgangen af maj 2019.

Ansættelsen rejser spørgsmålet om, hvordan man som forsker sikrer en objektivitet til emnet uden at være påvirket af en anklagerbaggrund, eksempelvis ved uforholdsmæssigt at tilgodese hensynet til politiets efterforskningsmuligheder over for hensynet til beskyttelsen af borgerens privatliv og rettigheder.

Min forskningsmæssige integritet er et aspekt, som jeg gennem hele ph.d.-forløbet har været opmærksom på og løbende har reflekteret over. Som værn mod en skævvridning af det forskningsmæssige fokus til politiets fordel, har jeg gennem hele forløbet prioriteret at formidle forskningsresultater og drøfte afhandlingens temaer med en bred kreds af eksterne interessenter, jf. ovenfor, hvilket har givet vigtige input til det videre arbejde.

Del 2 – Artiklerne

Oversigt over Artikel 1-6

Artikel 1: 'Hacking' og det digitale privatliv
Publiceret i Juristen, nr. 4/2018, s. 141-153.

Formål:
At analysere straffelovens § 263 om at skaffe sig uberettiget adgang til andres oplysninger i et informationssystem ('hacking'). Fokus er lagt på to typesituationer: Først den velmenende IT-'hacker', der tester systemer, og dernæst de sociale medier som nyt anvendelsesområde for 'hacking'-bestemmelsen. Analysen bidrager til forståelsen af, hvornår der er tale om privat område på internettet.

Metode:
Retsdogmatisk metode, med retspolitisk perspektivering.

Konklusion:
Artiklen viser, at grænsen for det digitale privatliv er ganske flydende, navnlig ved profiler og grupper på de sociale medier. Der opfordres til nærmere genovervejelse og præcisering af strafansvaret for 'hacking'.

Artikel 2: Logning af teledata i lyset af Tele2-dommen
Publiceret i Juristen, nr. 5/2017, s. 173-181.

Formål:
Artiklen behandler EU-Domstolens afgørelse i Tele2-sagen, som får betydning for både den danske logningspligt for teleselskaberne og for politiets adgang til teledata ved indgreb i meddelelseshemmeligheden. Særligt fokus er på, hvad der forstås ved "serious crime", som er det nye kriterium for politiets adgang til teledata som led i en efterforskning. Artiklen skal ses i sammenhæng med Artikel 3.

Metode:
Retsdogmatisk metode med retspolitisk perspektivering.
Et mindre, komparativt element ved sammenligning af den danske og svenske logningsregulering.

Konklusion:
EU-Domstolens har afvist den generelle logningspligt af al telekommunikation, og den danske logningspligt vil ikke kunne opretholdes i sin nuværende form. Der skal være tale om en 'målrettet' logning, og politiets adgang til de lagrede data, forudsætter at der efterforskes 'grov kriminalitet' mv.

Artikel 3: Retsplejelovens regulering af politiets adgang til teledata
Publiceret i Tidsskrift for Kriminalret, nr. 10/2017, s. 1240-1252.

Formål:
I fortsættelse af Artikel 2 undersøger denne artikel retsplejelovens regulering af indgreb i meddelelseshemmeligheden, i den kontekst af teledata, som blev aktualiseret med Tele2-sagen. Artiklen indgår i analysen af politiets tekniske indgreb på internettet.

Metode:
Retsdogmatisk metode med retspolitisk perspektivering.

Konklusion:
Der forestår en ganske vanskelig opgave med at sikre overensstemmelse med at indarbejde Tele2-dommens konklusioner i retsplejelovens regulering af tvangsindgreb. Desuden udfordres reglerne om indgreb i meddelelseshemmeligheden af tidens tand i forhold til udviklingen af nye digitale kommunikationsformer, hvilket navnlig ses i samspillet mellem indgreb i meddelelseshemmeligheden og ransagning.

Artikel 4: Politiets hjemmel til 'hacking' som led i en efterforskning
Publiceret i Tidsskrift for Kriminalret, nr. 7/2018, s. 814-823.

Formål:
Artiklen undersøger politiets hjemmel til 'hacking', som beror på et samspil mellem retsplejelovens regler om hemmelig ransagning, dataaflæsning og indgreb i meddelelseshemmeligheden. Desuden behandles den situation, hvor politiet ved undersøgelse af beslaglagte computere og mobiltelefoner vil kunne iværksætte en fremadrettet, online-overvågning, hvilket enten omfattes af beslaglæggelsen eller aktualiserer en hemmelig ransagning.

Metode:
Retsdogmatisk metode med retspolitisk perspektivering.

Konklusion:
På baggrund af Højesterets kendelse i U 2012.2614 H ser hemmelig ransagning nu ud til at være etableret som den almindelige hjemmel til politiets 'hacking'. Samspillet mellem de tre indgrebs-regelsæt forekommer ikke hensigtsmæssigt. Retsgrundlaget for overvågning via beslaglagte mobiltelefoner er uklart, hvorfor der bør skabes en klar regulering af denne form for efterforskning.

Artikel 5: Politiets infiltration på digitale platforme – set i et menneskeretligt perspektiv
Antaget til publicering i Nordisk Tidsskrift for Kriminalvidenskab, nr. 2/2019, planlagt udgivelse i september 2019.

Formål:
I artiklen analyseres efterforskningsmetoden infiltration, hvor politiet under dækker interagerer med borgeren. Metoden, der har sin baggrund i den fysiske verden, har ikke hidtil været reguleret. Det illustreres, hvordan infiltration kan foregå på digitale platforme.

Metode:
Retsdogmatisk metode med retspolitisk perspektivering.

Konklusion:
Infiltration kan i den digitale variant indeholde flere aspekter, der hver for sig kan udgøre indgreb i borgerens privatliv, korrespondance, ret til selvbestemmelse mv., jf. EMRK artikel 8. Der argumenteres for en regulering af infiltration.

Artikel 6: Politiagenter i et menneskeretligt perspektiv
Fremsendt til bedømmelse ved Juristen.

Formål:
Artiklen behandler retsplejelovens regulering af politiets agentvirksomhed, hvor fokus navnlig er på den processuelle ramme for iværksættelse af agentvirksomhed. I artiklen inddrages to nylige danske straffesager, hvori har indgået ret spektakulære agentaktioner.

Metode:
Retsdogmatisk metode med retspolitisk perspektivering.

Konklusion:
Der opfordres til en genovervejelse af den processuelle ramme for at sikre, at agentvirksomhed kun iværksættes og opretholdes til det strengt nødvendige for at sikre bevis for den kriminalitet, der efterforskes. Det anbefales at indføre advokatbeskikkelse og en begrænsning på varigheden af agentaktionen, som det kendes fra telefonaflytning mv. Et skærpet fokus på agentaktioner understøttes af praksis fra EMD, der har forholdt sig restriktivt til gentagne eller fortløbende agentaktioner, jf. EMRK artikel 6, stk. 1 om 'fair trial'.

Artikel 1: 'Hacking' og det digitale privatliv

(1)

(2)

(3)

(4)

(5)

(6)

(7)

(8)

(9)

(10)

(11)

(12)

(13)

Artikel 2: Logning af teledata i lyset af Tele2-dommen

(1)

(2)

(3)

(4)

(5)

(6)

(7)

(8)

(9)

Artikel 3: Retsplejelovens regulering af politiets adgang til teledata

(1)

(2)

(3)

(4)

(5)

(6)

(7)

(8)

(9)

(10)

Artikel 4: Politiets hjemmel til 'hacking' som led i en efterforskning

(1)

(2)

(3)

(4)

(5)

(6)

(7)

(8)

Artikel 5: Politiets infiltration på digitale platforme – set i et menneskeretligt perspektiv

(1)

(2)

(3)

(4)

(5)

(6)

(7)

(8)

(9)

(10)

(11)

(12)

(13)

(14)

(15)

(16)

(17)

(18)

(19)

(20)

(21)

(22)

(23)

(24)

(25)

(26)

(27)

Artikel 6: Politiagenter i et menneskeretligt perspektiv

(1)

(2)

(3)

(4)

(5)

(6)

(7)

(8)

(9)

(10)

(11)

(12)

(13)

(14)

(15)

(16)

(17)

(18)

(19)

(20)

(21)

(22)

(23)

(24)

(25)

(26)

(27)

Del 3 – Besvarelse af forskningsspørgsmål

Kapitel 1 Den overordnede retlige ramme for politiets hemmelige efterforskning på internettet

1. Retsplejeloven

Retsplejeloven, der udgør den overordnede retlige ramme for politiets efterforskning, indeholder ingen særlige bestemmelser, der relaterer sig til internettet. Det følger af § 742, stk. 2, at politiet efter anmeldelse eller af egen drift iværksætter efterforskning, når der er rimelig formodning om, at et strafbart forhold, som forfølges af det offentlige, er begået. Retsplejelovens kapitel 69-75 b indeholder en regulering af de straffeprocessuelle tvangsindgreb. Som anført i Artikel 5: *"Politiets infiltration på digitale platforme – set i et menneskeretligt perspektiv"*, har den såkaldt 'almindelige' efterforskning, som politiet kan foretage, og som ikke er udtrykkeligt reguleret som et tvangsindgreb, hjemmel i § 742, stk. 2.[107]

Aktualiseret af internettet og udviklingen af nye digitale efterforskningsmetoder er spørgsmålet, hvordan det afklares, om nye efterforskningsmetoder skal have hjemmel i lov, også betegnet som "det straffeprocessuelle legalitetsprincip."[108] Dette spørgsmål har været et gennemgående tema i artiklerne. I dette kapitel sammenfattes og udbygges dette tema.

2. Det straffeprocessuelle legalitetsprincip

Retsplejelovens regulering af de straffeprocessuelle tvangsindgreb – og at det netop er disse metoder, der er udvalgt til regulering – beror som tidligere nævnt på Gammeltoft-Hansens definition af et straffeprocessuelt tvangsindgreb, der afhænger af, om metoden realiserer "*en strafbar gerningsbeskrivelse rettet mod legeme, frihed, fred, ære eller privat ejendomsret*".[109] Udgangspunktet for definitionen er således, om politiets handlemåde ville indebære et strafansvar, hvis borgeren udførte samme handling. I så fald kræver politiets tvangsmæssige anvendelse af samme metode klar lovhjemmel. Modsætningsvist kan det af definitionen sluttes, at metoder, der ikke ville være strafbare for borgeren at anvende, ikke ved politiets anvendelse

[107] Artikel 5: *"Politiets infiltration på digitale platforme – set i et menneskeretligt perspektiv"*, pkt. 2

[108] Se Artikel 4: *"Politiets hjemmel til 'hacking' som led i en efterforskning"*, pkt. 2, Artikel 5: *"Politiets infiltration på digitale platforme – set i et menneskeretligt perspektiv"*, pkt. 1-2, og Artikel 6: *"Politiagenter i et menneskeretligt perspektiv"*, pkt. 3.

[109] Gammeltoft-Hansen: "*Straffeprocessuelle tvangsindgreb*", 1981, s. 44-45, samt "Om afgrænsningen af "straffeprocessuelle tvangsindgreb"", U1979B.1 ff.

har karakter af tvangsindgreb, og sådanne efterforskningsskridt kan derfor som udgangspunkt frit kan foretages; et særligt hjemmelsgrundlag kræves ikke.[110] Som eksempler nævner Gammeltoft-Hansen almindelig besigtigelse og skygning, der således ikke har karakter af tvangsindgreb.[111]

Gammeltoft-Hansens definition og systematik fra 1981 blev siden fulgt ved retsplejelovens regulering af tvangsindgrebene, herunder kategorisering i forhold til beskyttelsesinteressen, og de gennemgående krav ved alle indgreb: Kompetence- og formregler til indgrebet, og de tre krav til grovheden af den kriminalitet der efterforskes, mistankens styrke og indikationen/formålet med indgrebet.[112] Strafferetsplejeudvalget har "i det væsentlige tilsluttet sig" Gammeltoft-Hansens definition, som siden i vidt omfang er blevet fulgt ved reguleringen af nye tvangsindgreb.[113]

Gorm Toftegaard Nielsen har kritiseret Gammeltoft-Hansens definition, idet Toftegaard Nielsen ikke anser det for *"frugtbart at anskue politiets anvendelse af tvangsindgreb ud fra den teoretiske synsvinkel, at politiet principielt begår forbrydelser"*, og at der hermed *"formuleres et legalitetsprincip for politiet, som både i praksis og principielt er betydeligt snævrere end for resten af forvaltningen."*[114]

I stedet argumenterer Toftegaard Nielsen for, at politiets aktiviteter anskues som en del af den offentlige forvaltning, og at udgangspunktet for, hvornår der kræves lovhjemmel, søges ved de to forvaltningsretlige principper: Formelle lovs princip, som indebærer et forbud mod, at forvaltningens afgørelser strider mod loven, og legalitetsprincippet, hvoraf følger et krav om positiv lovhjemmel til at gøre indgreb i borgerens forhold, og hvor det gælder, at jo mere intensivt et indgreb er, desto større krav til lovhjemlens sikkerhed.[115]

Toftegaard Nielsen medgiver, at når det skal analyseres, *"hvilke indgreb, der er så alvorlige eller intensive, at de bør kræve klar lovhjemmel, vil man naturligvis komme*

---

[110] Gammeltoft-Hansen: "*Straffeprocessuelle tvangsindgreb*", 1981, s. 25, samt Birgitte Brøbech: "*Ulovligt tilvejebragte beviser i straffeprocessen*", 2003, s. 384.
[111] Gammeltoft-Hansen: "*Straffeprocessuelle tvangsindgreb*", 1981, s. 25.
[112] Gammeltoft-Hansen: "*Straffeprocessuelle tvangsindgreb*", 1981, samt Strafferetsplejeudvalgets Bet. 1023/1984, s. 12. ff.
[113] Jf. Bet. 1298/1995 om fotoforevisning, konfrontation, efterlysning og observation, s. 12. Se endvidere om definitionen, Michael Kistrup m.fl.: "*Straffeprocessen*", 2018, s. 443 ff., og Jørn Vestergaard: "*Straffeproces – grundtræk af dansk strafferetspleje*", 2018, s. 103 ff.
[114] Gorm Toftegaard Nielsen: "Hvad er et tvangsindgreb? Om straffeproces og forvaltningsret", Juristen 2005, s. 153.
[115] S. 156.

et langt stykke i retning af det rigtige, hvis man antager, at de overgreb, vi med straffebestemmelser har søgt at beskytte borgerne mod at blive udsat for fra en anden borger, sandsynligvis er så alvorlige, at vi for tilsvarende indgreb fra forvaltningen vil kræve lovhjemmel. Derfor er langt de fleste af de indgreb, Gammeltoft-Hansen når frem til som omfattet af sin definition, da også tvangsindgreb, som de fleste er enige om er så intensive, at de bør have klar lovhjemmel. Problemet opstår imidlertid i grænsetilfældene og især, hvis man vil slutte modsætningsvis fra de indgreb, der ikke er omfattet af definitionen, til, at de kan foretages uden lovhjemmel."[116]

Videre anfører Toftegaard Nielsen, at definitionen ikke er heldig i praksis, f.eks. i forhold til at anskue sigtelser som injurier, i stedet for at afgøre politiets videregivelse af oplysninger om sigtelse efter reglerne om tavshedspligt.[117] Desuden anfører Toftegaard Nielsen, at trangen til en udførlig og meget kompliceret lovregulering af tvangsindgrebene reelt har medført, at domstolene tvinges til at godkende tvangsindgreb, der *"ikke er hjemmel til i ordlyden af det komplicerede regelnet."*[118] Reguleringen af tvangsindgrebene har således efter Toftegaard Nielsens opfattelse nået grænsen for, hvor komplicerede efterforskningsregler politiet kan administrere i praksis.[119]

Birgitte Brøbech har anført, at forvaltningsretten stiller større krav til politiets hjemmel end procesretten gør med det af Gammeltoft-Hansen formulerede legalitetsprincip, og Brøbech argumenterer ligesom Toftegaard Nielsen for, at det straffeprocessuelle hjemmelsspørgsmål i højere grad analyseres med udgangspunkt i forvaltningsretten.[120] Gammeltoft-Hansens definition af et straffeprocessuelt tvangsindgreb, og hvornår der er krav om lovhjemmel, efterlader ingen plads til, at der i visse tilfælde kan være grund til at foretage en afvejning af reelle hensyn, så det eksempelvis er muligt at differentiere mellem, om det er en offentlig myndighed eller private borgere, der foretager de faktiske handlinger.[121] Uanset en gerning ikke er kriminaliseret for borgeren, kan der være grund til at lovregulere politiets brug af samme metode.

Som Brøbech konkluderer, er der ingen tvivl om, at Gammeltoft-Hansens indsats har haft stor betydning for, at de centrale tvangsindgreb i dag er reguleret i detaljer, og

[116] S. 156.
[117] S. 156 ff.
[118] S. 153.
[119] S. 159.
[120] Brøbech: "*Ulovligt tilvejebragte beviser i straffeprocessen*", 2003, s. 383 f.
[121] Brøbech: "*Ulovligt tilvejebragte beviser i straffeprocessen*", 2003, s. 395.

at dette er et vigtigt fremskridt for retssikkerheden i forhold til legalitetsprincippet.[122] Dog har Brøbech anført, at Gammeltoft-Hansens definition næppe er et hensigtsmæssigt instrument at benytte til at udskille de metoder, der ikke kræver lovhjemmel, idet definitionen "*er for håndfast og blåstempler efterforskningsmetoder, som en afvejning af reelle hensyn tilsiger, lovgiver bør tage stilling til, førend metoderne lovligt kan anvendes.*"[123]

Hans Gammeltoft-Hansen har i sit svar på Toftegaard Nielsens kritik navnlig henvist til den kontekst, som hans definition og systematik af straffeprocessuelle tvangsindgreb på daværende tidspunkt indgik i, hvor Strafferetsplejeudvalget stod over for en omfattende og kompliceret opgave med at fastlægge regler i retsplejeloven for den brogede mangfoldighed af indgreb.[124] Endvidere har Gammeltoft-Hansen henvist til, at udvalget i det væsentlige anvendte definitionen i en række betænkninger som fulgte i årene derefter, ligesom udvalget anvendte det andet element i Gammeltoft-Hansens forsøg på *"at skabe en vis teoretisk (og dermed forhåbentlig også praktisk) klarhed på feltet: Standardiseringen og gradueringen af især de materielle betingelser for alle tvangsindgreb (kriminalitets- mistanke- og indikationskrav, etc.)."*[125]

Endvidere har Gammeltoft-Hansen til Toftegaard-Nielsens kritik anført, at definitionen og systematikken kun angik en ganske bestemt facet af legalitetsprincippet, nemlig spørgsmålet om såkaldt kvalificeret hjemmel, idet Gammeltoft-Hansen anfører det som selvfølgeligt, at *"politiet som en forvaltningsmyndighed i al sin virksomhed er undergivet det almindelige hjemmelskrav – om at virksomheden ikke må stride mod lovbestemmelser, men derudover også i bredere forstand skal være legitimeret i lov eller anden anerkendt retskilde."*[126] I den henseende skal strafferetten ses som *"en assistance"* til at udfinde de konkrete kriterier for, hvornår der kræves kvalificeret hjemmel til politiets efterforskningsmetoder.[127] Gammeltoft-Hansens *"påstand er derfor ikke at definitionen og metoden er ideel, men at den er den mindst ringe til løsning af det store og ret så komplicerede problemfelt som reguleringen af de straffeprocessuelle tvangsindgreb og reglernes anvendelse udgør."*[128]

---

[122] Brøbech: "*Ulovligt tilvejebragte beviser i straffeprocessen*", 2003, s. 396.
[123] Brøbech: "*Ulovligt tilvejebragte beviser i straffeprocessen*", 2003, s. 396.
[124] Gammeltoft-Hansen: "Om definitionen af straffeprocessuelle tvangsindgreb" i "*Jurist uden omsvøb – festskrift til Gorm Toftegaard Nielsen*", af Annette Møller-Sørensen og Anette Storgaard (red.), 2007, s. 139-148, s. 140.
[125] S. 140.
[126] S. 141 f.
[127] S. 142.
[128] S. 146.

Med Toftegaard Nielsens sammenfatning af sine og Gammeltoft-Hansens synspunkter i "Straffesagens gang" fra 2016, synes parternes diskussion om definitionen nu at være afsluttet.[129]

Retstilstanden er nu, at retsplejelovens kapitel 69-75 b indeholder en regulering af en række straffeprocessuelle indgreb. Nye teknologiske muligheder kan betyde, at lovgiver tager stilling og fastlægger en udtrykkelig regulering. Mere sandsynligt er det, at de teknologiske nyskabelser viser sig i forbindelse med konkrete sager, hvor domstolene må tage stilling til metodernes lovlighed. Her vil domstolene skulle sammenholde den nye metode med det eksisterende regelsæt i retsplejeloven. Det interessante er, i hvor høj grad domstolene anvender analogier af de eksisterende hjemler til at omfatte de nye metoder. En snæver anvendelse af analogi, som det ses i den materielle strafferet, ville betyde, at domstolene i vidt omfang ville afskære brugen af nye teknologiske metoder, indtil lovgiver udtrykkeligt har taget stilling og fastsat betingelser for brugen.

For den videre behandling af det straffeprocessuelle legalitetsprincip, er det relevant i det følgende kort at introducere analogi som fortolkningsprincip, og her som forståelsesramme for den processuelle diskussion at inddrage den særlige, restriktive brug af analogi, som følger af straffelovens § 1 og EMRK artikel 7, stk. 1.[130]

2.1. Kort om analogi og det strafferetlige legalitetsprincip, jf. straffelovens § 1

Juridisk slutter man analogt, når man anvender en retsregel på et tilfælde, der ikke er omfattet af lovens ord, selv om der anlægges en meget vid sproglig forståelse af dem, såfremt de samme grunde taler for at følge lovens regel i begge tilfælde (der skal være "årsagernes lighed").[131]

Christina D. Tvarnø og Ruth Nielsen har anført, at man traditionelt antager, at der kan fortolkes udvidende eller sluttes analogt, hvis der foreligger årsagernes lighed og et retstomt rum, og for så vidt angår "årsagernes lighed" anføres, at de hensyn og principper, der begrunder reglen på det område, hvor den utvivlsomt gælder, gør sig gældende med samme eller stærkere styrke på det nye område.[132] Desuden må

[129] Gorm Toftegaard Nielsen: "*Straffesagens gang*", 2016, s. 84 ff.

[130] Senere i Kapitel 2, afsnit 3, forfølges det strafferetlige legalitetsprincip nærmere i relation til straffelovens 'hacking'-bestemmelse.

[131] Baumbach: "*Det strafferetlige legalitetsprincip – hjemmel og fortolkning"*, 2008, s. 396, med henvisning til Bo von Eyben: "*Juridisk ordbog*" (se 14. udgave, 2016, s. 47 f.)

[132] Christina D. Tvarnø og Ruth Nielsen: "*Retskilder og retsteorier*", 2017, s. 229 f. Se endvidere Peter Blume: "*Retssystemet og juridisk metode*", 2016, s. 302 f., og Carsten Munk-Hansen: "*Retsvidenskabsteori*", 2018, s. 306 ff.

der ikke være modstående hensyn, der gør, at det er uhensigtsmæssigt at slutte analogt.[133]

Ross har anført, at 'analogi' ofte *"opfattes som en ny, selvstændig retskilde ved siden af loven. Nogen principiel forskel mellem simpel udvidende fortolkning og analogislutning kan ikke påvises. Det første udtryk anvendes om de mere beskedne udvidelser, især når der foreligger specielle holdepunkter for, at et ord er anvendt med videre sigte end dets normale sproglige betydning dækker."*[134] Tvarnø og Nielsen har tilsluttet sig synspunktet om ikke at sondre mellem udvidende fortolkning og analogi, der antages at kunne anvendes under samme betingelser.[135]

Lovgiver har i straffelovens § 1 særligt taget stilling til brug af analogi på strafferettens område, idet bestemmelsen lyder: "*Straf kan kun pålægges for et forhold, hvis strafbarhed er hjemlet ved lov, eller som ganske må ligestilles med et sådant. (---)*"

Trine Baumbach har i *"Det strafferetlige legalitetsprincip – hjemmel og fortolkning"*, fra 2008, foretaget en grundig analyse af straffelovens § 1.[136] Om den strafferetlige analogi anføres af Baumbach, at ved "i straffelovens § 1 alene at tillade analogi i de tilfælde, hvor et forhold "*ganske* må ligestilles" med retsfaktum i en lovbestemmelse, har § 1 opstillet en analogibegrænsning, der afviger fra de almindelige regler om lovfortolkning."[137] Således betyder det strafferetlige legalitetsprincip efter straffelovens § 1 med Baumbachs ord, at "et faktisk begået forhold skal være en overtrædelse af en materiel lovbestemmelse, der kan udløse straf, eller også skal det faktisk begåede forhold *fuldstændig kunne ligestilles* med et forhold, som loven sanktionerer med straf (min fremhævning)."[138] Dette omtales af Baumbach som et

[133] Christina D. Tvarnø og Ruth Nielsen: "*Retskilder og retsteorier*", 2017, s. 230.
[134] Alf Ross: "*Ret og retfærdighed En indførelse i den analytiske retsfilosofi*", 1966, Nyt Nordisk Forlag Arnold Busck, s. 176 f. Se endvidere Preben Stuer Lauridsen: *"Retslæren"*, 1977, s. 323 ff., samt Sv. Gram Jensen: *"Almindelig retslære. En introduktion"*, 3. udgave, 1998, s. 137 f.
[135] Christina D. Tvarnø og Ruth Nielsen: "*Retskilder og retsteorier*", 2017, s. 229, med henvisning til Alf Ross: "*Ret og retfærdighed En indførelse i den analytiske retsfilosofi*", 1966, Nyt Nordisk Forlag Arnold Busck, s. 175 f.
[136] Se Baumbach: "*Det strafferetlige legalitetsprincip*", 2008, for så vidt den historiske baggrund s. 397 ff., den strafferetlige teori om analogi s. 409 ff., og retspraksis s. 414 ff. Se nærmere om det strafferetlige legalitetsprincip med litteraturhenvisninger, nedenfor i Kapitel 2, afsnit 3.
[137] Baumbach: "*Det strafferetlige legalitetsprincip*", 2008, s. 397 .
[138] Baumbach: "*Det strafferetlige legalitetsprincip*", 2008, s. 152 f.

krav om *"fuldstændig lovanalogi"*[139], og af Mads Bryde Andersen som *"analogiforbuddet."*[140]

Om brugen af analogi i strafferetten kan det ud fra Trine Baumbachs betragtninger sammenfattes, at der på den ene side er et hensyn til, at lige skal behandles lige, og når man slutter analogt, kan dette ses som et værn mod vilkårlighed og som et udslag af en retfærdighedstanke.[141] På den anden side er brugen af analogi set fra gerningsmandens retssikkerhedsperspektiv en kilde til retsusikkerhed og manglende forudsigelighed.[142] Endvidere anfører Baumbach, at også *"fra en demokratitilgang giver analogien problemer, idet det i udgangspunktet ikke kan være domstolens opgave at straffe forhold, som lovgiver ikke har kriminaliseret."*[143]

Det danske strafferetlige legalitetsprincip i straffelovens § 1 suppleres af legalitetskravet i EMRK artikel 7, stk. 1, 1. pkt. som lyder: *"Ingen kan kendes skyldig i et strafbart forhold på grund af en handling eller undladelse, der ikke udgjorde en forbrydelse efter national eller international ret på det tidspunkt, da den blev begået."*[144]

I dommen, *Kokkinakis mod Grækenland*, udtalte EMD, at bestemmelsen i artikel 7, stk. 1"… *embodies, more generally, the principle that only the law can define a crime and prescribe a penalty (nullum crimen, nulla poena sine lege) and the principle that the criminal law must not be extensively construed to an accused's detriment, for instance by analogy."*[145] Også i EMRK ses således et restriktivt værn mod udvidelse af straffebestemmelser som følge af analogi.[146]

---

[139] Baumbach: "*Det strafferetlige legalitetsprincip*", 2008, s. 259 og 395 ff., og samme anvendes af Vagn Greve: *"Det strafferetlige ansvar"*, 2004, s. 86. I "*Strafferet og Menneskeret*", 2014, foretrækker Baumbach dog betegnelsen "begrænset udvidet fortolkning", s. 81 og 116, af hensyn til EMD's indvendinger mod strafansvar som følge af analogi.

[140] Mads Bryde Andersen: "*IT-retten*", 2005, s. 724 f.

[141] Baumbach: "*Det strafferetlige legalitetsprincip*", 2008, s. 396.

[142] Baumbach: "*Det strafferetlige legalitetsprincip*", 2008, s. 396.

[143] Baumbach: "*Det strafferetlige legalitetsprincip",* 2008, s. 396.

[144] Artikel 7 indeholder en række retssikkerhedsmæssige elementer; i denne afhandling inddrages alene aspekter vedrørende materiel straffelovgivning og fortolkning. Således inddrages ikke tilbagevirkende kraft, eller hvorvidt en foranstaltning udgør "et strafbart forhold", ej heller spørgsmål om straffastsættelse, jf. artikel 7, stk. 1, 2. pkt., eller betragtninger i relation til artikel 7, stk. 2. I det følgende anvendes så vidt muligt betegnelsen "det strafferetlige legalitetsprincip" i relation til straffelovens § 1, og "legalitetskravet" i relation til EMRK artikel 7, stk. 1, 1. pkt.

[145] *Kokkinakis mod Grækenland*, dom af 25. maj 1993, pkt. 52.

[146] Om dette 'analogiforbud' sammenholdt med det danske krav om 'fuldstændig lovanalogi', se nærmere nedenfor Kapitel 2, afsnit 3.

Sammenfattende ses det strafferetlige legalitetsprincip, som følger af straffelovens § 1 og legalitetskravet i EMRK artikel 7, stk. 1, alene at give adgang til at straffe de af borgerens handlinger, som er udtrykkeligt kriminaliseret, eller som ved en snæver anvendelse af analogi findes at være omfattet af kriminaliseringen. Nærmere herom i Kapitel 2, afsnit 3, i relation til straffelovens 'hacking'-bestemmelse.

2.2. Retsplejelovens 'udtømmende katalog'

Hvis samme restriktive tilgang var gældende ved retsplejelovens regulering, ville det indebære, at politiet kun måtte anvende de metoder, der udtrykkeligt er reguleret eller kunne omfattes ved snæver anvendelse af analogi, hvorved afvigelser fra de regulerede metoder som hovedregel ville forudsætte ny regulering. Helt så enkel – og helt så restriktiv – er retstilstanden imidlertid ikke.

Det var Strafferetsplejeudvalgets ambition tilbage i Betænkning 1023/1984, så vidt muligt i retsplejeloven at opstille et "udtømmende katalog" over de straffeprocessuelle tvangsindgreb med tilhørende retlig regulering.[147] I forlængelse heraf var det Strafferetsplejeudvalgets opfattelse ved Betænkning 1298/1995, at det skulle være den overvejende hovedregel, at anvendelsen af straffeprocessuelle tvangsindgreb var forbudt, medmindre anvendelsen særlig var tilladt.[148] Dog var udvalget opmærksom på, at retsplejelovens bestemmelser næppe kunne udformes, så de til enhver tid udtømmende gør op med anvendelsen af alle straffeprocessuelle tvangsindgreb, og at der med tiden, navnlig i lyset af den teknologiske udvikling, kunne forekomme nye efterforskningsskridt, som ligeledes ville være omfattet af begrebet.[149]

2.3. Fortolkning i lyset af den teknologiske udvikling

I lyset af ambitionen om et "udtømmende katalog" er det interessant at se på, hvordan disse tvangsindgreb anvendes og fortolkes, når de udfordres af den teknologiske udvikling. Eksemplerne, der fremhæves i det følgende, er set over den sidste godt 20-årige periode. Først refereres de nye metoder, der allerede har været behandlet i artiklerne: Adgang til digitale brugerprofiler med rette kode, udvidet teleoplysning og teleobservation samt dataaflæsning. Herefter inddrages to efterforskningsmetoder, der ikke er indgået i artiklerne, således i afsnit 2.3.4.: Åbning af mobiltelefon med fingeraftryk, samt afsnit 2.3.5.: Gps-overvågning, hvorom der særligt er at bemærke, at denne metode for nylig er blevet reguleret i retsplejelovens § 791 a, stk. 5, nr. 2.

---

[147] Pkt. 1.2.

[148] Pkt. 1.5, hvor der henvises til Strafferetsplejeudvalgets tilkendegivelse i Bet. 1023/1984, s. 13.

[149] Bet. 1298/1995, pkt. 1.5.

2.3.1. Adgang til digitale brugerprofiler med rette kode

Højesterets kendelse om *politiets adgang til Facebook og Messenger-profiler med rette kode*, U 2012.2614 H, er et eksempel på domstolenes vurdering og kvalificering af en ny, digital efterforskningsmetode, som ikke er reguleret i retsplejeloven. Metoden indgik i analysen i Artikel 4: "*Politiets hjemmel til 'hacking' som led i en efterforskning.*"[150]

Sagen drejede sig om, hvordan dette indgreb i fravær af udtrykkelig lovregulering skulle vurderes i forhold til de lignende indgreb, dataaflæsning, hemmelig ransagning og indgreb i meddelelseshemmeligheden. Højesteret nåede frem til, at der var tale om gentagen, hemmelig ransagning, hvilket der var hjemmel til i efterforskningen af den konkrete narkotika-forbrydelse, jf. retsplejelovens § 799. Byretten og landsretten havde godkendt indgrebet i medfør af reglerne om dataaflæsning.

Det fremgår af referatet i ugeskriftet, at Højesteret i kendelsen brugte formuleringen: *"Højesteret finder, at indgrebene har karakter af gentagne hemmelige ransagninger, som kan foretages med hjemmel i retsplejelovens § 793, stk. 1, nr. 1, jf. § 799."*

2.3.2. Udvidet teleoplysning og teleobservation

Disse to efterforskningsmetoder blev behandlet i Artikel 3: *"Retsplejelovens regulering af politiets adgang til teledata."* Herfra kan refereres, at *teleoplysning* angår "oplysning om, hvilke telefoner eller andre tilsvarende kommunikationsapparater der sættes i forbindelse med en bestemt telefon eller andet kommunikationsapparat, selv om indehaveren af dette ikke har meddelt tilladelse hertil, jf. § 780, stk. 1, nr. 1". En variant heraf, *udvidet teleoplysning*, indebærer, at teleoplysninger indhentes for et nærmere angivet geografisk område i relation til de mobiltelefoner, der befinder sig i området. Fra tidligere retspraksis var der eksempler på, at et sådant indgreb ikke blev tilladt, hvilket var baggrunden for lovændringen i 2001, hvor indgrebet blev udtrykkeligt reguleret i retsplejelovens § 780, stk. 1, nr. 4 og § 781.[151]

Før lovændringen havde Højesteret taget stilling til udvidet teleoplysning i U 1997.1021 H, hvor politiets efterforskning angik en bombe med sprængstof, som var blevet placeret i en gade i København. Politiet anmodede om, at det blev pålagt to mobiltelefonselskaber at give oplysning om, hvilke telefoner, der inden for et bestemt tidsrum havde været sat i forbindelse med hinanden via de pågældende selskabers sendemaster, der geografisk dækkede en bestemt adresse og et område, der lå inden for 1 km's afstand. Byretten fandt, at indgrebet vedrørte et meget vidt og ubestemt antal telefoner, og at der ikke var bestemte grunde til at antage, at der

[150] Se endvidere Lene Wacher Lentz: "Hemmelig ransagning og brevstandsning i den digitale virkelighed", Juristen 1/2016.

[151] Udvidet teleoplysning blev reguleret ved lov nr. 465 af 7. juni 2001.

fra disse telefoner var givet meddelelser af betydning for efterforskningen, og som følge heraf fandtes betingelserne for teleoplysning i retsplejelovens bestemmelse om teleoplysning, jf. § 781, stk. 1. Landsretten tillod indgrebet, som man fandt omfattet af reglerne om teleoplysning. Højesteret stadfæstede imidlertid byrettens kendelse, da der ikke var mulighed for nærmere afgrænsning af samtaleregistreringer vedrørende mobiltelefoner, og derfor fandt Højesteret ikke, at der var fornøden hjemmel i § 780, stk. 1, nr. 3, til at indhente de teleoplysninger, som anklagemyndigheden havde begæret.[152]

I relation til *teleobservation*, der handler om at følge en mobiltelefons geografiske placering ud fra hvilke telemaster, den gør brug af, blev metoden reguleret i retsplejeloven i 2006.[153] Inden da måtte Højesteret tage stilling til denne nye efterforskningsmetode i U 2003.137 H. Byretten havde fundet, at indhentelsen af sådanne oplysninger var omfattet af observationsreglerne i retsplejelovens § 791 a, stk. 3, men havde vurderet, at forbrydelsens grovhed ikke opfyldte betingelserne herfor, hvorfor den konkrete anmodning ikke kunne imødekommes. Landsrettens flertal havde derimod fundet, at der ikke var tale om et straffeprocessuelt indgreb, og at politiet derfor uden retskendelse kunne indhente oplysningerne. Højesteret lagde vægt på, at oplysningerne skulle anvendes i tilknytning til politiets skygning af personen, hvorfor Højesteret fandt, at indgrebet kunne "sidestilles med observation", jf. retsplejelovens § 791 a, og – da oplysningerne ikke kunne stadfæste en persons færden så præcist, at den kunne lokaliseres til en bolig eller andre husrum – at indgrebet var omfattet af retsplejelovens § 791 a, stk. 2, og ikke stk. 3. De tre retsinstanser var dermed kommet til tre forskellige resultater.

2.3.3. Dataaflæsning

Denne efterforskningsmetode blev behandlet i Artikel 4: *"Politiets hjemmel til 'hacking' som led i en efterforskning",*[154] hvorfra det om baggrunden for bestemmelsen i retsplejeloven kan refereres, at politiet i U 2001.1276 H havde anmodet om rettens tilladelse til at installere et edb-program ("snifferprogram") i en mistænkts edb-udstyr for at gøre sig bekendt med, hvad der blev skrevet på computeren, der var installeret i en lejlighed, med hjemmel i retsplejelovens § 791 a, stk. 3 om observation. Når begæringen ikke angik observation af personer i bolig eller husrum, afslog byretten at give tilladelse til indgrebet efter § 791 a, stk. 3, idet indgrebet ikke var omfattet af bestemmelsens fuldstændige analogi. Landsrettens flertal tillod indgrebet

[152] Af retspraksis ses endvidere, at landsretten i U 1999.320 Ø tillod et sådant indgreb, som man fandt behørigt afgrænset i forhold til antal meddelelser og samtaler, der blev involveret, mens landsretten i den senere dom, U 2001.245 Ø, afslog et sådant indgreb.

[153] Lov nr. 542 af 8. august 2006.

[154] Se endvidere Lene Wacher Lentz: "Hemmelig ransagning og brevstandsning i den digitale virkelighed", Juristen 1/2016.

under henvisning til, at indgrebet var muliggjort af ny teknologi, og at det kunne sidestilles med de foranstaltninger, der fremgik af § 791 a, stk. 3 og ikke findes mere indgribende end disse, hvorefter flertallet fandt indgrebet omfattet af bestemmelsen eller dennes analogi.[155]

Højesteret fandt, at der ikke var hjemmel i § 791 a, stk. 3 til en sådan observation, men vurderede, at indgrebet "mest nærliggende" kunne sidestilles med gentagen hemmelig ransagning, hvorefter Højesteret stadfæstede byrettens kendelse om ikke at tillade indgrebet. Med til forståelsen af Højesterets kendelse hører, at retstilstanden på daværende tidspunkt var således, at der ikke var hjemmel i retsplejelovens § 799 til på forhånd at tillade mere end én hemmelig ransagning inden for den i kendelsen anførte periode, hvilket Højesteret havde fastslået i U 1999.985 H. Muligheden for gentagne – og eventuelt et ubestemt antal – *hemmelige ransagninger* blev først indført i retsplejelovens § 799, stk. 3 i 2002.[156] Højesterets kendelse om "snifferprogrammet" i U 2001.1276 H blev senere medvirkende til indførelsen af en udtrykkelig bestemmelse om dataaflæsning i retsplejelovens § 791b.[157]

2.3.4. Åbning af mobiltelefon med fingeraftryk

I U 2019.1304 H godkendte Højesteret i to sager, at politiet havde ransaget de mistænktes mobiltelefoner ved at tvinge de pågældende til at åbne telefonerne ved brug af deres fingeraftryk, der blev presset ned på mobiltelefonernes fingeraftrykslæsere. Fremgangsmåden var tilladt af by- og landsretten efter ransagningsreglerne, dog fandt landsretten, at der tillige var tale om legemsbesigtigelse i form af optagelse af fingeraftryk, jf. retsplejelovens § 792, stk. 1, nr. 1, hvilke betingelser dog også var opfyldt i de konkrete sager.

Spørgsmålet for Højesteret angik, om der var hjemmel til et sådant indgreb, og om indgrebet kunne foretages uden forudgående retskendelse. Højesteret fandt, at den magt, der kortvarigt havde været anvendt ved at anbringe tommelfingeren på mobiltelefonen, så indholdet på telefonen kunne udlæses, var nødvendig for at gennemføre ransagningen, og at magtanvendelsen derfor som et accessorium var omfattet af det straffeprocessuelle tvangsindgreb, der var hjemlet i retsplejelovens bestemmelser om ransagning af bl.a. aflåste genstande.

Dette aspekt om 'accessorium' blev uddybet af Højesteret: *"Det svarer til, at politiet under en ransagning af en mistænkts bolig midlertidigt fratager den mistænkte nøglen til boligen med magt for at skaffe sig adgang hertil. Også i andre sammenhænge*

[155] Dissens i landsretten for at stadfæste byrettens kendelse.
[156] Lov nr. 378 af 6. juni 2002, se hertil Artikel 4: *"Politiets hjemmel til 'hacking' som led i en efterforskning"*, pkt. 3.2., og Lene Wacher Lentz: "Hemmelig ransagning og brevstandsning i den digitale virkelighed", Juristen nr. 1/2016, pkt. 4.4.2.
[157] Lovforslag nr. 35 af 13. december 2001, pkt. 3.4.1., til lov nr. 378 af 6. juni 2002.

kan et straffeprocessuelt tvangsindgreb i visse tilfælde udgøre et accessorium til et andet indgreb, f.eks. politiets kortvarige frihedsberøvelse af en person ved legemsindgreb og politiets mulighed for at skaffe sig adgang til en lokalitet i forbindelse med opsætning af aflytningsudstyr."

Højesteret, der således tillod fremgangsmåden med hjemmel i ransagningsreglerne, fandt ikke, at reglerne om legemsbesigtigelse tillige skulle være opfyldt. Desuden tiltrådte Højesteret, at der havde været risiko for, at politiets mulighed for at skaffe sig oplysninger fra de mistænktes mobiltelefoner ville gå tabt, hvorfor indgrebene kunne foretages uden forudgående retskendelse.[158]

2.3.5. Gps-overvågning

Som endnu en ny teknologisk efterforskningsmetode, politiet har taget i brug, og som har resulteret i en nylig lovregulering, kan ses metoden at montere pejlingsudstyr/GPS-udstyr på mistænktes biler. Ved U 1996.1496 V tog Vestre Landsret stilling til politiets anbringelse af elektronisk sporingsudstyr *uden på* en mistænkts bil, hvilket landsretten konkluderede var skygning under anvendelse af tekniske hjælpemidler, og at der ikke ved indgrebet var *"realiseret nogen strafbar krænkelse rettet mod tiltaltes legeme, frihed, fred, ære eller private ejendomsret."* Som landsretten anførte i begrundelsen: *"Selvom der er tale om et efterforskningsskridt, der eventuelt kunne gøres til genstand for en nærmere regulering, finder landsretten ikke, at nævnte skridt kræver lovhjemmel og dermed heller ikke forudgående indhentelse af retskendelse."* Byretten havde ligeledes fundet, at der var tale om skygning under anvendelse af tekniske hjælpemidler, der ikke krævede retskendelse.

En variant af efterforskningsmetoden, hvor udstyret anbringes *inde i* bilen, tog Højesteret senere stilling til i U 2000.2476 H, hvor Højesteret anførte: *"…den omstændighed, at pejlingen forudsætter, at der sker en indtrængen i bilen, ikke i sig selv medfører, at et efterforskningsskridt – der uden på en bil kan foretages uden tilladelse – end ikke kan foretages med rettens tilladelse uden særskilt lovregulering. Pejling må anses for en særlig form for observation"* og dermed *"anses for at være omfattet af eller sidestillet med observationsbegrebet i retsplejelovens § 791 a."* Nærmere bestemt fandt Højesteret, at indgrebet var omfattet af § 791 a, stk. 2. At der er tale om vanskelige vurderinger ses af, at byretten ifølge domsreferatet havde tilladt indgrebet efter retsplejelovens § 791 a, stk. 3, mens landsretten var nået frem til, at indgrebet ikke kunne tillades, bl.a. under henvisning til, at det fremtrådte som et nyt straffeprocessuelt tvangsindgreb, der måtte antages at kunne få almindelig anvendelse, og som derfor burde forudsætte en lovregulering.[159]

---

[158] Denne 'accesorium'-problematik indgår senere i afhandlingen i relation til kryptering, jf. Del 3, Kapitel 3.

[159] Om disse domme om gps-overvågning, se Gorm Toftegaard Nielsen: "Hvad er et tvangsindgreb? Om straffeproces og forvaltningsret", Juristen nr. 5/2005, s. 158 f.

Denne retstilstand, hvor der sondres mellem montering uden på eller inde i bilen, var gældende ret frem til 1. januar 2019, hvor der blev indført en udtrykkelig bestemmelse om politiets gps-overvågning i retsplejelovens § 791 a, stk. 5, nr. 2. Uden at Gammeltoft-Hansens definition af tvangsindgreb nævnes i Straffelovrådets Betænkning 1563/2017 om freds- og ærekrænkelser, virker det stadig til at være denne definition, der udgør grundlaget for rådets overvejelser, hvorved der sikres en parallelitet mellem strafferetten og strafferetsplejens tvangsindgreb.[160] Således foreslog Straffelovrådet i Betænkningen at indføre en straffebestemmelse om ulovlig overvågning i straffelovens § 264 b, således *at "den, som uberettiget ved hjælp af en gps eller et andet lignende apparat registrerer en andens færden, straffes med bøde eller fængsel indtil 6 måneder."*[161] Herefter anførte Straffelovrådet: "*Det vil være en konsekvens af den nye bestemmelse, at politiets anvendelse af sporings- og pejlingsudstyr som omhandlet i bestemmelsen i forbindelse med efterforskningen af strafbare forhold fremover i alle tilfælde vil være at anse som et straffeprocessuelt tvangsindgreb, som skal have hjemmel i retsplejeloven*."[162] I den forbindelse gjorde Straffelovrådet rede for dagældende ret, jf. ovenfor, som tog hensyn til, om senderen var anbragt uden på eller inde i køretøjet. Justitsministeriet var enig i Straffelovrådets overvejelser.[163] Sammenhængen mellem borgerens strafansvar og de straffeprocessuelle tvangsindgreb træder således tydeligt frem her, helt i overensstemmelse med Hans Gammeltoft-Hansens definition.[164]

Straffelovrådets forslag blev senere fulgt i relation til straffelovens § 264 b, og ved samme lov blev retsplejelovens ændret, således at § 791 a, stk. 5 om teleobservation også kom til at indeholde hjemmel til, at politiet "på anden måde ved hjælp af en gps eller et andet lignende apparat (kan) registrere 1) en mistænkts færden eller 2) en anden persons færden, hvis den pågældende har tilknytning til en mistænkt eller til samme køretøj eller ejendom som en mistænkt eller lignende", jf. stk. 5, nr. 2.[165]

Fra et menneskeretligt perspektiv kan det konstateres, at EMD allerede i *Uzun mod Tyskland*, dom af 2. september 2010, havde fastslået, at politiets gps-overvågning af en mistænkt udgjorde et indgreb i hans privatliv, jf. artikel 8, stk. 2, uden at EMD i

---

[160] Jf. Artikel 5: *"Politiets infiltration på digitale platforme – set i et menneskeretligt perspektiv"*, pkt. 3.1.
[161] Bet. 1563/2017, s. 112 ff. og s. 198.
[162] S. 115.
[163] Lovforslag nr. 20 af 3. oktober 2018, pkt. 2.5.3.
[164] Jf. Artikel 5: *"Politiets infiltration på digitale platforme – set i et menneskeretligt perspektiv*", pkt. 3.1.
[165] Jf. Lov nr. 1719 af 27. december 2018 om ændring af straffeloven, retsplejeloven, lov om erstatningsansvar og medieansvarsloven (freds- og ærekrænkelser mv), trådt i kraft 1. januar 2019. Se om lovændringerne, lovforslag nr. 20 af 3. oktober 2018.

begrundelsen foretog nogen sondring af, om gps-udstyret var anbragt inde i eller uden på bilen. Ej heller inddrages spørgsmålet, hvorvidt samme metode efter tysk ret var kriminaliseret for borgeren at foretage. Domstolen lagde til grund, at der var tale om overvågning af den mistænkte, hvilket havde stået på i ca. tre måneder, og at politiet havde brugt oplysninger derfra til efterforskningen mod ham.[166] Dog bemærkede EMD, at gps-overvågning var mindre indgribende end de metoder, hvor der også var billed- eller lyd-overvågning.[167] Spørgsmålet for Domstolen var herefter, om indgrebet var i overensstemmelse med loven efter tysk ret i relation til artikel 8, stk. 2, og i den henseende forelå ikke en krænkelse i den konkrete sag.[168]

Eksemplet med gps-overvågning bekræfter det danske straffeprocessuelle udgangspunkt, som fortsat sker i overensstemmelse med Hans Gammeltoft-Hansens definition, dog må dette til stadighed sammenholdes med udviklingen af de menneskeretlige standarder, som Danmark ved inkorporering af EMRK er forpligtet af. I relation til gps-overvågning ses anvendelsen af Gammeltoft-Hansens definition at relatere sig til, om gps-anordningen monteres uden på eller inde i bilen, og beskyttelsesinteressen synes herefter at fokusere på privatlivet 'inde i bilen', når gps-anordningen frit kan monteres uden på bilen uden lovregulering. Derimod ses EMD's tilgang mere præcist at forstå det indgreb i privatlivet, der sker ved, at den enkelte borger bliver udsat for målrettet, detaljeret, langvarig, teknologisk overvågning af sin færden. Som anført af Toftegaard Nielsen, ville man i forvaltningsretten næppe være i tvivl om, at en sådan overvågning døgnet rundt af, hvor borgernes biler befinder sig, er et indgreb, der kræver lovhjemmel.[169]

2.4. Sammenfatning af den hidtidige retspraksis

Som det ses, giver retspraksis et noget broget billede af, hvordan domstolene vurderer nye teknologiske efterforskningsmetoder, hvilket understreges af, at de forskellige retsinstanser, byret, landsret og Højesteret, ofte ses at komme til forskellige resultater.

Den restriktive fortolkning, der ville ligne analogiforbuddet i straffelovens § 1, ville resultere i, at hvis en metode ikke er udtrykkeligt reguleret i retsplejeloven på anvendelsestidspunktet, kan domstolene som hovedregel ikke tillade metoden anvendt. En sådan fortolkning ses kun sjældent anvendt.

I de tilladte indgreb, kan man notere sig ordlyden i Højesterets begrundelser, eksempelvis i U 2012.2614 H, at politiets adgang til Facebook- og Messenger-profilerne

[166] Pkt. 49-53.
[167] Pkt. 52.
[168] Pkt. 64-74.
[169] Toftegaard Nielsen: "Hvad er et tvangsindgreb? Om straffeproces og forvaltningsret", Juristen nr. 5/2005, s. 159.

havde "*karakter af* gentagne hemmelige ransagninger", i U 2003.137 H, hvor Højesteret fandt, at teleobservation kunne "*sidestilles med* observation", og i U 2000.2476 H hvor Højesteret udtalte, at "Pejling må *anses for en særlig form for* observation. Pejling ved anvendelse af udstyr, hvis installation indebærer et straffeprocessuelt indgreb, må derfor anses for at være omfattet af eller sidestillet med observationsbegrebet i retsplejelovens § 791 a." Her er ikke tale om en sproglig eller præciserende fortolkning, men i stedet en udvidende fortolkning beroende på "årsagernes lighed", selv om Højesteret synes at være tilbageholdende med at anvende ordet analogi i sine begrundelser.

Sammenfattende for retspraksis ses, at udvidende fortolkning i vidt omfang anvendes som led i en konkret vurdering af hver enkelt metode. Hovedindtrykket er, at der i de fleste tilfælde sker en forholdsvis pragmatisk vurdering i forhold til det eksisterende katalog af tvangsindgreb, og hvad den konkrete nye metode 'ligner mest'. I flere tilfælde ses sammenligningen at ske i forhold til observationsreglerne, som indeholder en graduering af betingelserne.[170]

Ét er disse teknologiske variationer over fænomenet 'skygning med hjælpemidler', noget ganske andet er, når spørgsmålet angår nye spektakulære metoder, såsom snifferprogrammet i U 2001.1276 H, som Højesteret fandt skulle sidestilles med gentagen hemmelig ransagning, som der ikke var hjemmel til på daværende tidspunkt. Eller der er tale om større nye, intensive indgreb, som udvidet teleoplysning i forhold til et større geografisk område, som Højesteret ikke fandt hjemmel til i U 1997.1021 H. Denne metode angår meddelelseshemmeligheden, som er restriktivt beskyttet (Grundlovens § 72, EMRK artikel 8 samt retsplejelovens kapitel 71), og Højesterets afvisning af metoden må ses i lyset af, at en stor mængde ikke-mistænkte herved ville blive involveret i indsamlingen af kommunikationsdata, og at der ikke i retsplejeloven var noget sammenligneligt indgreb.

2.5. De bagvedliggende hensyn i strafferetten og straffeprocessen

Som fælles, overordnede hensyn for både strafferetten og straffeprocessen står helt centralt hensynet til borgerens retssikkerhed, og at reguleringen skal modvirke vilkårlighed og magtmisbrug. Som konkluderet ovenfor er der ikke tale om, at straffelovens snævre adgang til analogi af straffebestemmelserne, jf. straffelovens § 1, også er gældende for reguleringen af de straffeprocessuelle tvangsindgreb, hvor lovgiver har tilkendegivet, at retsplejeloven så vidt muligt skal udgøre et 'udtømmende katalog' over politiets tvangsindgreb, og hvor domstolene sammenligner og tillader indgreb ud fra metoden, intensiteten og friere overvejelser.

[170] Om observationsreglerne i retsplejelovens § 791 a, stk. 1-3, nedenfor Kapitel 3, afsnit 3.

Forklaringen på forskellen skal desuden ses i lyset af formålet og de bagvedliggende hensyn, der relaterer sig til henholdsvis straffeloven og straffeprocessen. Formålet med straffelovens bestemmelser er groft sagt at adfærdsregulere borgeren med trussel om straf,[171] mens formålet med straffeprocessen er at fastlægge, hvordan et strafbart forhold efterforskes og retsforfølges, hvor der i den forbindelse kan påføres borgeren forskellige indgreb (i privatliv, ejendom mv.)

Begrundelsen for "analogiforbuddet" i straffelovens § 1 er hensynet til borgerens retssikkerhed, der tilgodeses ved en klar og forudsigelig retstilstand, således at borgeren kan indrette sin opførsel, så han ikke gør noget strafbart (og bliver straffet for det). Dog har Trine Baumbach påpeget, at en meget restriktiv fortolkning af straffeloven, som tilgodeser gerningsmandens retssikkerhed, ikke altid tilgodeser den forurettede i sagen, der kan opleve, at det "legislative værn" svigter, når gerningen ikke straffes som følge af straffelovens § 1 og EMRK artikel 7.[172]

I straffeprocessen ses af retspraksis, at nye teknologiske metoder til en vis grad accepteres efter fortolkning (analogi) af eksisterende hjemler, når der i forhold til intensiteten er lighed. Her spiller det formentlig også ind, at retsbeskyttelsen tilgodeses ved, at indgrebet sker efter retskendelse, hvor der tages konkret stilling til indgrebets efterforskningsmæssige berettigelse. Denne tilgang til at tillade nye metoder, der tilgodeser hensynet til at nå frem til den materielle sandhed om, hvad der er foregået, beror på en tillid til politi, anklagemyndighed og domstole, og heri ligger også en tiltro til, at der ikke sker magtmisbrug. Regulering af efterforskningsmetoder tilgodeser borgerne i bred forstand, der herved generelt sikres mod vilkårlige, uproportionale og uberettigede indgreb, men hensynet til den konkrete gerningsmand er her nedtonet i forhold til, hvad der gør sig gældende inden for den materielle strafferet. Således indgår det ikke i overvejelserne for den straffeprocessuelle regulering, om gerningsmandens har mulighed for at forudsige, hvad politiet kan og må, så han har mulighed for at indrette sig, så han ikke bliver opdaget.

Straffeprocessens bagvedliggende hensyn og de retlige rammer, hvor indgrebene i vidt omfang sker efter retskendelse, er således en vigtig kontekst til forståelsen af,

[171] Her betones strafferettens præventive formål både i forhold til den enkelte borger (specialprævention) og i form af almenprævention (generalprævention), se en gennemgang og diskussion af forskellige straffeteorier i Baumbach: "*Strafferet og menneskeret*", 2014, s. 54 ff., endvidere Waaben: "*Strafferettens almindelige del – Ansvarslæren*", 6. reviderede udgave ved Lars Bo Langsted, 2015, s. 37 ff., Gorm Toftegaard Nielsen: "*Strafferet I – Ansvaret*", 2013, s. 19 f., og Vagn Greve: "*Det strafferetlige ansvar*", 2004, s. 19-48.

[172] Jf. Baumbach: "*Strafferet og menneskeret*", 2014, s. 17.

hvorfor domstolene ikke anlægger samme restriktive tilgang til nye efterforskningsmetoder, som det sker inden for strafferetten i medfør af straffelovens § 1 og EMRK artikel 7.

3. Det menneskeretlige perspektiv

Gammeltoft-Hansens definition resulterer i et forholdsvis snævert område, der skal reguleres, når der ved et tvangsindgreb er tale om *"en foranstaltning, der efter sit almindelige formål udføres som led i en strafforfølgning, og hvorved der realiseres en strafbar gerningsbeskrivelse rettet mod legeme, frihed, fred, ære eller privat ejendomsret."*[173] Altså at forstå således, at politiets metode omsat til borgerens adfærd ville realisere et strafansvar. I de tilfælde, hvor en konkret metode efter definitionen udgør et tvangsindgreb, skal metoden ifølge Gammeltoft-Hansen have udtrykkelig hjemmel i retsplejeloven.

Reguleringen efter EMRK artikel 8 er væsentligt anderledes, idet EMD anlægger en bred forståelse af, hvad der kan karakteriseres som et indgreb i privatlivet, jf. artikel 8, stk. 1, eksempelvis når der tales om retten til selvbestemmelse og retten til at udvikle relationer.[174] Til gengæld følger det af stk. 2, at indgreb i retten til privatliv skal ske "i overensstemmelse med loven", hvilket dog ikke efter EMD' praksis nødvendigvis skal være formel lov. Også uskreven ret eller domspraksis kan udgøre det retlige grundlag for et indgreb, når blot dette grundlag er tilgængeligt for borgeren, og retstilstanden kan siges at være forudsigelig for borgeren.[175] Dog stiller EMD skærpede krav til hjemmelens klarhed, når der er tale om alvorlige indgreb, såsom ransagning og beslaglæggelse, og ligeledes når der er tale om hemmelige indgreb, eksempelvis i meddelelseshemmeligheden.[176]

Ved at sammenholde Gammeltoft-Hansens definition med reguleringen i EMRK vil resultatet formentlig være det samme for så vidt angår de alvorligste indgreb: en klar hjemmel til politiets indgreb i retsplejeloven, dog således at EMD ofte ses at give ret detaljerede anvisninger for den regulering, der kræves, som eksempelvis i form af 'minimumsgarantier' ved telefonaflytning.[177]

---

[173] Gammeltoft-Hansen: "*Straffeprocessuelle tvangsindgreb*", 1981, s. 44-45, se hertil Artikel 4: "*Politiets hjemmel til 'hacking' som led i en efterforskning*", pkt. 2.
[174] Jf. Artikel 5: *"Politiets infiltration på digitale platforme – set i et menneskeretligt perspektiv"*, pkt. 4.2.2. ff.
[175] Jf. Artikel 5: "*Politiets infiltration på digitale platforme – set i et menneskeretligt perspektiv*", pkt. 4.3.
[176] Jf. Artikel 4: "*Politiets hjemmel til 'hacking' som led i en efterforskning*", pkt. 2.
[177] Se hertil Artikel 5: "*Politiets infiltration på digitale platforme – set i et menneskeretligt perspektiv*", pkt. 4.3.

Forskellen på de to tilgange til politiets efterforskning træder tydeligst frem ved de mindre alvorlige efterforskningsmetoder, hvor EMRK kan kræve et retsgrundlag, der ikke ville være resultatet efter Gammeltoft-Hansens definition, eksempelvis i forhold til politiets indsamling og registrering af personoplysninger. Også metoden 'infiltration' kan anskues i relation til indgreb i privatlivet med et legalitetskrav, jf. artikel 8, stk. 2, hvilket behandles i Artikel 5: *"Politiets infiltration af digitale platforme – set i et menneskeretligt perspektiv."*

Ligeledes i forhold til metoden agentvirksomhed ses en forskel i forhold til den danske straffeprocessuelle tilgang og EMD's tilgang til metoden. Om agentvirksomhed i forhold til definitionen af et straffeprocessuelt tvangsindgreb anførte Gammeltoft-Hansen, at agentvirksomhed falder uden for definitionen, idet der ikke sker indgreb i en individuel beskyttelsesinteresse, og at en sådan i givet fald måtte beskrives som *"retten til ikke at blive udsat for fristelse til at foretage kriminelle handlinger"*, hvilket ikke er udtryk for et retsbeskyttet gode.[178] Imidlertid fandt Gammeltoft-Hansen, Strafferetsplejeudvalget og efterfølgende lovgiver, at efterforskningsmetoden rummede principielle betænkeligheder, der gjorde, at metoden skulle reguleres på samme måde som de straffeprocessuelle tvangsindgreb.[179]

Som anført i Artikel 6: *"Politiagenter i et menneskeretligt perspektiv*", har EMD i tilknytning til artikel 6, stk. 1 om retfærdig rettergang fastsat en række retsgarantier for denne efterforskningsmetode, og disse retlige standarder udvikles løbende i Domstolens praksis. Perspektivet fra EMRK og Domstolens fortolkning er således, om agentvirksomhed påvirker tiltaltes ret til retfærdig rettergang ved, at han af politiet provokeres til en forbrydelse, han ellers ikke ville have begået. Denne tilgang er helt upåvirket af, om metoden opfylder en definition om et straffeprocessuelt tvangsindgreb, og om samme fremgangsmåde ville være strafbar for borgeren.

Som det påpeges i Artikel 6: *"Politiagenter i et menneskeretligt perspektiv*", må opmærksomheden løbende følge retsudviklingen på dette område i Domstolens praksis, hvor nye aspekter kan fordre danske lovgivningsmæssige tiltag for at sikre overensstemmelse, uagtet man tilbage i 1986 mente at have tilgodeset retssikkerheden ved en regulering af agentvirksomhed, selv om det ud fra Gammeltoft-Hansens definition af et straffeprocessuelt tvangsindgreb ikke var påkrævet at gøre dette. På den baggrund kan det undre, at det i foråret fremsatte forslag (L 197) om udvidet adgang til agentvirksomhed ved strafbare forhold begået ved brug af internettet,

[178] Gammeltoft-Hansen: "*Straffeprocessuelle tvangsindgreb*", 1981, s. 70.
[179] Gammeltoft-Hansen: "*Straffeprocessuelle tvangsindgreb*", 1981, s. 66, og artiklen "'Agent controlleur'" i Tidsskrift for Rettsvitenskap, 1984, s. 126 f., og som medlem af Strafferetsplejeudvalget i Bet. 1023/1984, s. 151 f., samt lovforslag nr. 8 af 2. oktober 1985, pkt. 1., jf. hertil Artikel 6: *"Politiagenter i et menneskeretligt perspektiv."*

ikke indeholdt bemærkninger relateret til menneskeretlige aspekter, jf. Artikel 6: *"Politiagenter i et menneskeretligt perspektiv*", pkt. 5.[180]

Hans Gammeltoft-Hansens definition har hidtil været et pejlemærke for lovgiver i relation til, hvilke af politiets efterforskningsmetoder der skulle reguleres, men i lyset af EMD's anvisninger om regulering af indgreb efter artikel 8, stk. 2, er lovgiver nødt til at have et bredere perspektiv på, hvilke af politiets metoder, der skal have et retligt grundlag. Affattelsen af politilovens § 2 a, stk. 2 om indsamling af offentligt tilgængelige oplysninger er et eksempel på, at lovgiver sikrer udtrykkelig overensstemmelse med EMD-praksis. Således må opmærksomheden konstant være på EMD og de retningslinjer, der i tilknytning til retspraksis fastlægges på dette område.

Som anført i Artikel 5: "*Politiets infiltration på digitale platforme – set i et menneskeretligt perspektiv*",[181] tager den menneskeretlige vurdering efter artikel 8, stk. 2 ikke udgangspunkt i, hvorvidt samme handling er strafbar for borgeren, men Domstolen anlægger sin egen vurdering af handlingens karakter i forhold til borgerens privatliv, korrespondance mv. Det menneskeretlige perspektiv støtter således det af Toftegaard Nielsen og Brøbech anførte, om at spørgsmålet om lovhjemmel til politiets efterforskningsmetoder i højere grad må afgøres efter det forvaltningsretlige legalitetsprincip ud efter konkrete analyser, og på den baggrund bør lovgiver i højere grad frigøre sig fra Gammeltoft-Hansens definition og det deraf følgende, meget snævre, legalitetsprincip.

Gorm Toftegaard Nielsen har som del af sin kritik af Gammeltoft-Hansens definition af et straffeprocessuelt tvangsindgreb anført, at domstolene som praktisk konsekvens af definitionen *"tvinges til at godkende tvangsindgreb, der ikke er hjemmel til i ordlyden af det komplicerede regelnet."*[182] Hertil kan man blot konstatere, at 'regelnettet' ikke forventes at blive mindre i årene fremover, snarere mere fintmasket med påvirkningen fra EMRK og Domstolens praksis, der i højere grad kræver et retligt grundlag for en række mindre indgribende efterforskningsmetoder og en nuanceret stillingtagen til anvendelsen heraf. Formentlig vil der ikke i fremtiden være meget af politiets efterforskning, der på en eller anden måde berører borgeren, der blot kan forventes henført under den almindelige efterforskningshjemmel i § 742, stk. 2.

[180] Lovforslag nr. 197 fremsat den 13. marts 2019, der imidlertid bortfaldt i forbindelse med folketingsvalget i juni 2019.
[181] Pkt. 3.1., med henvisning til Toftegaard Nielsen: "Hvad er et tvangsindgreb? Om straffeproces og forvaltningsret", Juristen, 2005, s. 160, samt Artikel 4: "*Politiets hjemmel til 'hacking' som led i en efterforskning*", s. 815.
[182] Toftegaard Nielsen: "Hvad er et tvangsindgreb? Om straffeproces og forvaltningsret", Juristen, 2005, s. 153 ff.

Det straffeprocessuelle legalitetsprincip med konstant inddragelse af EMRK-aspekter må anvendes af lovgiver til løbende at sikre, at den danske retsplejelov er i overensstemmelse hermed, navnlig når nye efterforskningsmetoder tages i brug. Heri ligger også en vejledning til retsanvenderne, som kan have tillid til, at de menneskeretlige aspekter på overordnet plan er i overensstemmelse med lovgivningen.[183] Uagtet denne generelle overensstemmelse, må også domstolene, og anklagere og forsvarere, ved afgørelsen af konkrete sager være opmærksomme på de menneskeretlige, straffeprocessuelle aspekter, hvor nye domme fra EMD kan føje nye aspekter til, f.eks. som det er tilfældet på området for agentvirksomhed, og hvor dansk ret må inddrage disse retlige standarder.

4. Sammenfatning vedrørende det straffeprocessuelle legalitetsprincip

Til forskningsspørgsmålet om, hvordan det straffeprocessuelle legalitetsprincip og definitionen af det straffeprocessuelle tvangsindgreb skal anskues i lyset af EMRK, gives der ikke noget entydigt nyt svar på dette. Hvilke efterforskningsmetoder, der skal reguleres i retsplejeloven beror på en konkret vurdering, hvori indgår en flerhed af hensyn: En sammenligning med straffelovens regulering, jf. Hans Gammeltoft-Hansens definition, kan være ét parameter, som i mange situationer fortsat kan være relevant at inddrage, hvilket bekræftes ved denne artikels tema om 'hacking' og sondringen mellem offentligt og privat område. Et andet aspekt i vurderingen er forvaltningsretlige overvejelser, jf. Gorm Toftegaard Nielsen, og i dette perspektiv ville eksempelvis gps-overvågning af biler kræve regulering. Endelig indgår i vurderingen de forskellige aspekter relateret til EMRK, navnlig artikel 6 og 8, og Domstolens praksis, hvori Konventionens rettigheder dynamisk fortolkes og nyudvikles.

Disse mange aspekter og hensyn gør, at det ikke er muligt at videreudvikle Hans Gammeltoft-Hansens definition til en ny begrebsfastsættelse, der kan fungere som en praktisk anvendelig målestok til lovgiver om, hvilke efterforskningsmetoder der kræver regulering i retsplejeloven. Allerede som følge af den righoldige praksis og løbende retsudvikling fra EMD ville dette ikke en gangbar løsning. I stedet må lovgiver opfordres til et øget fokus på nye efterforskningsmetoder, der muligt skal reguleres, ny retspraksis, hvor domstolene har kvalificeret nye metoder ved fortolkning af eksisterende indgrebshjemler, og som giver anledning til regulering (eksempelvis U 2012.2614 H) samt praksis fra EMD, der skal indarbejdes i den danske retstilstand, som det eksempelvis ses ved agentvirksomhed.

[183] Pernille Boye Koch: "Lovgivers rolle som fortolker af internationale retskilder – på hvilken måde gælder menneskerettighederne i Danmark?", Tidsskrift for Rettsvitenskap, vol. 132, 1/2019, s. 3-50.

Som følge af den teknologiske udvikling og menneskerettighedernes indflydelse på dansk ret, kan konstateres en tendens til øget regulering af politiets efterforskningsmetoder, således at en stadig mindre del betragtes som 'almindelig efterforskning', som politiet uden nærmere regulering kan foretage i efterforskningen af strafbare forhold. En øget 'retliggørelse' giver fastere rammer for politiets efterforskningsmæssige metoder og dermed bedre beskyttelse af borgeren og dennes retssikkerhed. Ulempen kan dog blive en høj grad af kompleksitet i regelsættet og et mindre skønsmæssigt spillerum til politiet i det daglige, omskiftelige efterforskningsarbejde.

5. Praktiske aspekter ved politiets ibrugtagning af nye, digitale efterforskningsmetoder

Når politiet tager nye digitale efterforskningsmetoder i brug, er der ikke i Danmark en egentlig godkendelsesprocedure eller validering af sådanne nye tiltag, ud over hvad der måtte følge af den forvaltningsretlige kultur i politi og anklagemyndighed, hvor overordnede instanser eller ekspertise internt i organisationen tages med på råd.

Det følger af retsplejelovens § 96, at de offentlige anklageres opgave er i forbindelse med politiet at forfølge forbrydelser efter reglerne i retsplejeloven. Videre følger det af stk. 2, at de offentlige anklagere skal fremme enhver sag med den hurtighed, som sagens beskaffenhed tillader, og derved ikke blot påse, at strafskyldige drages til ansvar, men også at forfølgning af uskyldige ikke finder sted. Straffeprocessuelt kan det siges at følge af § 96, at politi og anklagemyndighed skal agere lovligt og retssikkerhedsmæssigt korrekt, samt loyalt varetage både hensynet til almenheden og til den enkelte borger, der omfattes af efterforskningen.

Ved nye efterforskningsmetoder kan anklagemyndigheden vælge at anmode om rettens tilladelse til at bruge metoden i efterforskningen af en konkret sag, eventuelt med henvisning til, at metoden er en teknologisk variant af en af de retsplejelovens tvangsindgreb, som man derfor ønsker en kendelse om. Men det sker også, at metoden forelægges for retten med det formål at indhente en "nul-kendelse", hvorved forstås, at man får rettens ord for, at en given efterforskningsmetode ikke kræver retskendelse. Præcedens af disse nul-kendelser kan dog diskuteres, navnlig hvis der ikke ved retsmødet har været beskikket en forsvarsadvokat for en sigtet eller en indgrebsadvokat, jf. retsplejelovens § 784. Sådanne advokaters involvering ville kunne give kontradiktion og mere principielle diskussioner om lovligheden af nye efterforskningsmetoder, og den manglende inddragelse af en modpart til anklagemyndigheden bevirker, at der ikke er mulighed for kære på vegne af de berørte borgere. Dermed resulterer rettens prøvelse af spørgsmålet ikke i en trykt afgørelse, der vil kunne diskuteres i bredere kredse.

I de situationer, hvor der ikke udtrykkeligt er taget stilling til en metodes lovlighed eller nærmere regulering i retsplejeloven, er det også en mulighed, at politiet uden videre

tager metoden i brug, eventuelt ud fra en formodning om, at metoden ligger inden for den almindelige efterforskning, der kan foretages med hjemmel i retsplejelovens § 742, stk. 2. Herefter vil det være op til forsvareren, at søge sig oplyst om de efterforskningsmetoder, politiet har anvendt i den konkrete sag, og eventuelt at indbringe efterforskningens lovlighed for retten, jf. retsplejelovens § 746, eller at problematisere efterforskningen under hovedforhandlingen.

I sådanne tilfælde vil en stor del af ansvaret og initiativet for, at domstolene får mulighed for at tage stilling til den nye efterforskningsmetode komme til at ligge på forsvarerens skuldre.[184]

Her må man huske på forsvarerens rolle i en straffesag. En forsvarer beskikkes af retten til at bistå en klient, der er sigtet for et strafbart forhold. Bliver forsvareren opmærksom på, at politiet har brugt en ny efterforskningsmetode på internettet, må forsvareren overveje, om det er værd at gå videre med ved domstolene. Dette afhænger af forsvarerens og den sigtedes prioritering, og af hvad de sammen skønner er bedst for klienten. Der er mange modhensyn, der gør, at en forsvarer ikke nødvendigvis prioriterer et formelt slagsmål om en ny, teknologisk efterforskningsmetode: Det vil tage tid at afklare metodens lovlighed, når spørgsmålet skal prøves i retten, eventuelt i flere instanser. Forsvareren og klienten må også tænke på, om de øvrige beviser i sagen alligevel vil medføre, at klienten bliver dømt. Det er klienten, der ender med sagsomkostningerne, hvis han bliver dømt i sin straffesag, og han er måske mere interesseret i at få en hurtig dom og komme i gang med afsoningen.

Det må også spille ind i forsvarerens overvejelser, at der ved danske domstole er en tradition for, at selvom politiets efterforskning skulle ske at få kritik, vil dette oftest ikke medføre, at det bevis, der fremkom ved den kritiserede eller ulovlige efterforskning, afskæres fra at indgå i sagen og blive brugt mod den tiltalte. I de fleste tilfælde vil retten tillade beviset ført i straffesagen. Selvom en forsvarer kan ske at få medhold af retten i, at en ny efterforskningsmetode er kritisabel eller måske endda ulovlig, vil det derfor næppe ændre på sagens udfald for klienten.[185]

En stor del af initiativet er dermed lagt på forsvareren for, at domstolene kan tage stilling til nye digitale efterforskningsmetoder. Dette indebærer en fare for, at politi og anklagemyndighed i et vist omfang tager nye metoder i brug, som en forsvarer

[184] Dette og de næste tre afsnit er et lettere omarbejdet uddrag af "Efterforskningens grænser på internettet", af Lene Wacher Lentz, s. 139, bidrag til antologien " *Eksponeret – Grænser for privatliv i en digital tid*", af Rikke Frank Jørgensen og Birgitte Kofod Olsen (red.), 2018.

[185] Om domstolenes tilbageholdenhed med at afskære ulovligt tilvejebragte beviser, se Michael Kistrup m.fl.: *"Straffeprocessen"*, 2018, s. 27 f. og 678 ff., samt Birgitte Brøbech: *"Ulovligt tilvejebragte beviser i straffeprocessen"*, 2003, s. 401 ff.

ikke bliver opmærksom på eller bare ikke prioriterer at tage et retligt opgør om. Dermed får domstolene kun i begrænset og sporadisk omfang mulighed for at tage stilling til sådanne nye metoder, fastlægge betingelserne for brugen og anlægge de nye skillelinjer for afvejningen mellem hensynet til den enkelte borger over for politiets efterforskning af forbrydelsen.

Dette aspekt om forsvarerens rolle taler for en påpasselighed med blot at overlade det til domstolene selv at regulere og udvikle retlige rammer for politiets nye teknologiske efterforskningsmetoder. I stedet må erkendes, at her er nogle ganske vigtige grænseflader mellem borger og myndighed, som lovgiver i vidt omfang må tage ansvar for at regulere.

De to følgende kapitler følger op på de to typetilfælde for politiets hemmelige efterforskning, idet der på baggrund af tidsskrifts-artikel 1-6 sammenfattes og perspektiveres, først i forhold til reguleringen af politiets 'tekniske indgreb' og dernæst i forhold til det 'menneskelige indgreb.' I relation til begge typer efterforskning påvises problematiske aspekter, hvilket giver anledning til flere retspolitiske overvejelser.

Kapitel 2 Straffelovens bestemmelse om 'hacking' som pejlemærke for politiets efterforskning

1. Relevans for politiets efterforskning

Internettet giver en række udfordringer, når det skal fastlægges, hvilke 'datasystemer' der er private, og hvortil adgangen er uberettiget. I Artikel 1: "'*Hacking' og det digitale privatliv*" analyseres straffelovens 'hacking'-bestemmelse, jf. straffelovens § 263, for nærmere at klarlægge disse grænser i et strafferetligt perspektiv.

Udgangspunktet for at analysere straffelovens 'hacking'-bestemmelse i relation til politiets hemmelige efterforskning på internettet, beroede på overvejelser ud fra Hans Gammeltoft-Hansens definition af et straffeprocessuelt tvangsindgreb. Således at forstå, at den grænse for det digitale privatliv, som borgeren ifølge 'hacking'-bestemmelsen skulle respektere, også måtte gælde for politiets tekniske adgang til et datasystem. Politiets forcering af denne grænse ville dermed udgøre et straffeprocessuelt tvangsindgreb, der skulle have hjemmel i retsplejeloven.

Uanset de indvendinger mod en for skematisk brug af Gammeltoft-Hansens definition, der tidligere er nævnt, er behandlingen af 'hacking'-bestemmelsen i en strafferetlig kontekst fortsat relevant i forhold til at afdække, hvor grænsen går for borgerens digitale privatliv, og hvor borgeren kan have en forventning om privatliv. Dette er også væsentlige aspekter at inddrage i en straffeprocessuel kontekst, hvor grænserne for politiets efterforskning på internettet skal afdækkes.

I denne afhandling udelades en række andre aspekter, der relaterer sig til det 'digitale privatliv', således navnlig reguleringen af videregivelse af private meddelelser, billeder mv., jf. straffelovens § 264 d, og databeskyttelsesreguleringen, som er central for den enkeltes beskyttelse mod uberettiget registrering og behandling af personoplysninger. Som Henrik Udsen har påpeget, er der et overlap, hvor både straffelovens bestemmelser om freds- og ærekrænkelser og databeskyttelsesreguleringen kan finde anvendelse, og hvor en del af disse straffelovsovertrædelser kan anskues som kvalificerede brud på reglerne om behandling af personoplysninger.[186] Udsen redegør for de to væsensforskellige regelsæt og understreger vigtigheden af at sikre en overensstemmelse.

[186] Henrik Udsen: "Digitale freds- og ærekrænkelser – mellem strafferet og persondataret" i "*Festskrift til Mads Bryde Andersen*", af Henrik Udsen, Jan Schans Christensen, Jesper Lau Hansen, Torsten Iversen og Linda Nielsen (red.), 2018, s. 121-146.

2. Sammenfattende og opfølgende om straffelovens 'hacking'-bestemmelse

'Hacking'-bestemmelsens grundlæggende gerningsindhold blev fastlagt i straffeloven i 1985.[187] Det må alene betragtes som sproglig modernisering, at beskrivelsen af det angrebne system i 2004 blev ændret fra "et anlæg til elektronisk databehandling" til "et informationssystem". De øvrige ændringer i 2004 i relation til 'hacking'-bestemmelsen angik alene strafferammer og ordlyden af de skærpende omstændigheder i stk. 3.[188]

'Hacking'-bestemmelsen er senest ændret ved lov nr. 1719 af 27. december 2018, hvor "informationssystem" blev ændret til "datasystem", ligesom 'hacking'-bestemmelsen blev flyttet fra straffelovens § 263, stk. 2 til stk. 1.[189] Det bemærkes i lovforslaget, at der alene er tale om sproglige ændringer, ingen indholdsmæssig ændringer.[190]

Som det fremgår af Artikel 1: "*'Hacking' og det digitale privatliv*", er 'hacking'-bestemmelsen udfordret af navnlig to nye digitale typesituationer, som den nylige Betænkning 1563/2017 ikke har forholdt sig til. Den ene situation angår den 'velmenende IT-hacker', hvor spørgsmålet bliver, hvor langt ind i (eller hvor tæt på) informationssystemet, man skal være for at have fået 'adgang'. Må man "tage i døren for at se, om den er åben", uden at blive straffet for forsøg på uberettiget adgang? Først ved at prøve at få adgang, opdager man, om det er et privat og beskyttet system, og der er det måske for sent. Som det ses i skattemappesagen, U 2015.345 Ø, skal der alligevel være tale om en kvalificeret indsats, før der straffes for forsøg. Dette sammenlignet med 2017-Betænkningens eksempel om en medarbejder, der alene af nysgerrighed og uden et videregående forsæt til brug eller videregivelse tilgår oplysninger, der ikke er relevante for arbejdet, og hvor domstolene ifølge Straffelovrådet bør være tilbageholdende med at anse adgangen for uberettiget.[191] Hvad man konkret foretager sig, og hvor hurtigt, man 'trækker sig ud af systemet igen' efter at have fået adgang, vil derfor i konkrete straffesager få betydning for, om der er skaffet uberettiget adgang og navnlig for, om der er forsæt hertil.

Status er formentlig om IT-'hackeren', at det vil være i orden at undersøge systemet nok til at konstatere, om det er et privat og beskyttet system. Mere vanskeligt er det

[187] Lov nr. 229 af 6. juni 1985, der byggede på forslag fra Straffelovrådets Bet. 1032/1985 om datakriminalitet.
[188] Lov nr. 352 af 19. maj 2004.
[189] Lov nr. 1719 af 27. december 2018 om ændring af straffeloven, retsplejeloven, lov om erstatningsansvar og medieansvarsloven (freds- og ærekrænkelser m.v.), trådt i kraft den 1. januar 2019.
[190] Lovforslag nr. 20 af 3. oktober 2018, specielle bemærkninger til § 263.
[191] Straffelovrådets Bet. 1563/2017 om freds- og ærekrænkelser, s. 61.

at vurdere er de tilfælde, hvor man nærmere undersøger, præcist hvordan et system er sikret, hvis man er helt bekendt med, at man ikke har berettiget adgang. I denne gråzone må formodningen være, at man ikke må begynde at udfordre sikkerheden for at få adgang, eller vise at man kan, hvilket kan realisere et forsøg på uberettiget adgang, jf. byrettens dom i sagen om IT-'hackeren', som også anført i Artikel 1: "*'Hacking' og det digitale privatliv*", pkt. 4.

Den anden type-situation, der udfordrer 'hacking'-bestemmelsen, angår de sociale medier, som udgør en ny kontekst for 'hacking'-bestemmelsen, og spørgsmålet er om politi, anklagemyndighed og domstolene er parate til de udfordringer, som sådanne sager giver. Sagen om ekskærestens Facebook-'hacking' i U 2017.247 V viser, at der var mange omstændigheder ved gerningen, som ikke – i hvert fald ikke ifølge domsreferatet – blev udtrykkeligt behandlet ved den noget kortfattede proces, som en tilståelsessag udgør. Her tænkes på spørgsmål om samtykke fra forurettede og kutyme for sådan adgang, og i det lys også forskellige aspekter relateret til tiltaltes forsæt.

Som det fremgår af Artikel 1: "*'Hacking' og det digitale privatliv*", pkt. 5.2., er de sociale medier i vidt omfang kendetegnet ved, at det er den menneskelige tilladelse, der udgør 'sikkerhedsforanstaltningen' til lukkede eller halvoffentlige 'zoner'. Vi giver hinanden adgang til private grupper på baggrund af de oplysninger, vi har om den anmodende person, hvilket afstemmes med 'zonens' betingelser for medlemskab. Disse betingelser kan variere betydeligt, spændende lige fra at alle interesserede kan få adgang, til mere eller mindre diffuse krav, som i artiklen eksemplificeres ved krav om bestemt slægtsskab, eller at man har en bestemt sygdomsdiagnose. Det er hidtil uafklaret i retspraksis, hvordan en straffesag ville stille sig, hvis en person har fået adgang til et lukket område på de sociale medier på baggrund af svigagtige oplysninger. Som anført i artiklen, må det først afklares, hvorvidt svigagtige oplysninger er årsagen til, at der er givet adgang, idet der ved vurdering af eventuelt strafansvar kan ses bort fra svigagtige oplysninger, som administrator ikke har tillagt betydning. I de tilfælde hvor det kan lægges til grund, at der er denne 'årsagsforbindelse' mellem svig og adgang, sættes i artiklen fokus på en mulig internetadfærd, hvor man 'lyver en lille smule', og hvilken strafferetlig betydning, det skal have.

'Hacking'-bestemmelsen i straffelovens § 263, stk. 1 består af nogle meget brede begreber – "uberettiget", "adgang" og "datasystem" – som udfordres af de nye digitale scenarier, og det er vanskeligt at forudsige, hvor præcist det strafbare område går. Dette kan være problematisk for borgerens retssikkerhed.

For at vurdere om 'hacking'-bestemmelsens anvendelsesområde er for bredt, i lyset af at en række forskelligartede 'hacking'-scenarier på de sociale medier i realiteten kan rummes heri, inddrages i det følgende de begrænsninger til en kriminalisering, som følger af det strafferetlige legalitetsprincip, jf. straffelovens § 1 og legalitetskravet i EMRK artikel 7, stk. 1.

3. Den strafferetlige legalitetsprincip, jf. straffelovens § 1

Det følger af straffelovens § 1, at *"straf kun kan pålægges for et forhold, hvis strafbarhed er hjemlet ved lov, eller som ganske må ligestilles med et sådant."*[192] Legalitetsprincippet, som det behandles i det følgende, kan her adskilles i to dele: Først at forholdet skal have lovhjemmel, hvor spørgsmålet bliver, om formuleringen af bestemmelsen er tilstrækkelig præcis til, at borgeren ved, hvad der gælder. Dernæst om lovhjemlen ved en udvidet fortolkning (analogi) også kan straffe andre forhold, der ikke er omfattet af ordlyden, hvilket kort blev berørt ovenfor i Kapitel 1, afsnit 2.1.

Spørgsmålet om, hvorvidt en straffebestemmelse er tilstrækkelig præcis til, at borgeren kan vide, hvilken gerning, der medfører straf, kan illustrereres med det klassiske tyske, teoretiske eksempel om en straffebestemmelse med ordlyden, *"Jeder Schurke wird bestraft"*, hvor gerningsindholdet er formuleret så bredt, at ingen får nogen vejledning om, hvilken form for skurkagtig adfærd, der sigtes til.[193]

Vurderingen af en straffebestemmelse som en præcis vejledning til borgeren kan anskues i forhold til, om straffebestemmelsen er tilstrækkelig 'klar', eller om det er 'forudsigeligt' for borgeren, hvad der kan straffes for. Om disse begreber har Baumbach anført, at begrebet 'klarhed' refererer til en bestemmelses ordlyd, og at idealet der ligger heri tilsiger *"at straffebestemmelser skal være formuleret så præcist, at borgeren blot ved at læse loven skal kunne få en sikker viden om det strafbares område – altså hvad der er forbudt og strafbart, og hvad der er tilladt."*[194] Begrebet 'forudsigelighed' refererer ifølge Baumbach *"ikke til selve retskilden og ordlyden af*

---

[192] Om det strafferetlige legalitetsprincip og analogi, se Baumbach: "*Det strafferetlige legalitetsprincip*", 2008, og Baumbach: "*Strafferet og menneskeret*", 2014, s. 115 ff. Se endvidere bl.a. Thomas Elholm, Morten Niels Jakobsen og Lasse Lund Madsen: "*Kommenteret straffelov Almindelig del*", 2019, s. 104 ff., Knud Waaben: "*Strafferettens almindelige del – Ansvarslæren*", 6. reviderede udgave ved Lars Bo Langsted, 2015, s. 102 ff., Gorm Toftegaard Nielsen: "*Strafferet I – Ansvaret*", 2013, s. 43 ff., Vagn Greve: *"Det strafferetlige ansvar"*, 2004, s. 85 ff., Knud Waaben: "Lovkravet i strafferetten", Nordisk Tidsskrift for Kriminalvidenskab, 1994, s. 130-139, Stephan Hurwitz: "*Den danske kriminalret Almindelig del, 4. reviderede udgave ved Knud Waaben"*, 1971, s. 87 ff., samt Bernhard Gomard: "Analogi i strafferetten" i "*Festskrift til Alf Ross*" af Mogens Blegvad, Max Sørensen, Isi Foighel, Jørgen Trolle og A. Vinding Kruse (red.), 1969, s. 125-152.

[193] Trine Baumbach: "*Det strafferetlige legalitetsprincip*", 2008, s. 157, med henvisning til Ernst Beling: *"Die Lehre vom Verbrechen"*, Tübingen 1906, s. 22, og Dan Frände: *"Den straffrättsliga legalitetsprincippet"*, 1989, s. 241.

[194] Baumbach: "*Strafferet og menneskeret*", 2014, s. 121.

denne, men til den endelige fortolkning af det pågældende retsgrundlag."[195] Som anført af Baumbach skal gerningsindholdet og hjemlen til at pålægge straf fremgå af loven, men der stilles ikke i straffelovens § 1 *"noget direkte krav af kvalitativ art til de lovregler, der kriminaliserer handlinger. Heller ikke grundloven indeholder regler om straffelovens kvalitet."*[196]

Generelt fremgår det af Justitsministeriets Vejledning om lovkvalitet (juni 2018), pkt. 2.1., at der gælder et krav om klarhed i lovgivningen, navnlig når loven giver myndighederne mulighed for at foretage indgreb over for borgerne i form af f.eks. straf, konfiskation mv., hvorfor der her er et særligt behov for forudsigelighed i retstilstanden. *"Også i øvrigt er det et grundlæggende element i lovkvalitet, at enhver, som lovteksten henvender sig til, så vidt muligt let skal kunne læse og forstå den. Lovforslag skal således affattes klart, systematisk, let læseligt og pædagogisk. En godt og klart affattet lov er en nødvendig forudsætning for en ensartet retsanvendelse og dermed for forudsigelighed og retssikkerhed."*[197]

I forhold til den anden del af legalitetsprincippet, var spørgsmålet, hvorvidt en lovhjemmel ved en udvidet fortolkning (analogi) også kunne straffe andre forhold, der ikke er omfattet af ordlyden.[198]

I tilknytning til straffelovens § 1 har Baumbach anført, at det ved konkrete vurderinger af, om der kan sluttes analogt fra en strafbestemmelse, vil være afgørende, om der er et hul i lovgivningen, og om der er høj grad af formålslighed og lighed med retsfakta, og om denne lighed er så stor, at der er lige så stærke grunde til at straffe i det nye tilfælde, som i de allerede kendte forhold, der er omfattet af straffebestemmelsen.[199] Desuden skal domstolene være opmærksomme på, at der ikke sker en utilsigtet udglidning af en bestemmelses anvendelsesområde, når der ved det første forhold sluttes analogt i forhold til en straffebestemmelse, og der ved et senere andet forhold sluttes analogt i forhold til det første forhold, selvom det andet forhold måske ikke har fuld tilstrækkelig lighed med det oprindelige anvendelsesområde for straffebestemmelsen.[200]

Gorm Toftegaard Nielsen har rejst spørgsmålet, om det forhold, at domstolene ved vurdering af beviser for tiltaltes skyld skal lade enhver rimelig tvivl komme ham til

[195] Baumbach: "*Strafferet og menneskeret*", 2014, s. 121.
[196] Baumbach: "*Strafferet og menneskeret*", 2014, s. 121, i samme retning Gorm Toftegaard Nielsen: *"Strafferet 1- Ansvaret"*, 2013, s. 38 f.
[197] Justitsministeriets Vejledning om lovkvalitet (juni 2018), pkt. 2.1.
[198] Jf. ovenfor Kapitel 1, afsnit 2.1.
[199] Baumbach: "*Det strafferetlige legalitetsprincip*", 2008, s. 434 ff.
[200] Baumbach: "*Det strafferetlige legalitetsprincip*", 2008, s. 436.

gode (in dubio pro reo), også fører til, at dette princip af hensyn til tiltaltes retssikkerhed skal følges ved fortolkningen af loven. Således at forstå, at domstolene af hensyn til tiltaltes retssikkerhed altid skal vælge det mindste strafbare område. Toftegaard Nielsen har hertil anført, at der ikke kan opstilles et sådant fortolkningsprincip i dansk ret, allerede begrundet i straffelovens § 1, der som straffehjemmel accepterer fuldstændig analogi.[201]

I det følgende illustreres dansk strafferetspraksis om analogi som følge af teknologiske nyskabelser. Herefter inddrages praksis fra EMD i relation til § 7, stk. 1, som bl.a. stiller krav om, at retstilstanden er forudsigelig for borgeren.

3.1. Dansk retspraksis om analogi som følge af ny teknologi

Der er en righoldig retspraksis om anvendelse af analogi i strafferetten.[202] Her skal alene fremhæves tre trykte domme, der er udtryk for domstolenes vurdering af analogi som straffehjemmel i sager, hvor den kriminelle handling er begået ved hjælp af nye teknologiske løsninger. Opmærksomheden henledes dog på det af Trine Baumbach anførte om, at hensynet til tiltaltes mulighed for at forudsige de strafferetlige konsekvenser af sine handlinger formentlig er tillagt stigende betydning gennem årene, og at det derfor er *"rimeligt at antage, at ældre domme, hvor der er sket domfældelse på baggrund af en analogi, ikke nødvendigvis kan anses for retningsgivende i dag."*[203]

I dommen, refereret i U 1940.156 Ø, blev den tiltalte straffet efter en analogi af den tidligere § 263, der dengang kun kriminaliserede retsstridige brevåbninger, til også at dække hemmelig aflytning ved hjælp af lytteudstyr.[204] Om dommen har Tvarnø og Nielsen anført, at til fordel for en analogi fra brud på brevhemmeligheden til telefonaflytning taler, at formålet i begge tilfælde er at beskytte privatlivets fred, og at fordelen ved en analogifortolkning netop vil være, at man ved løbende fortolkning kan ajourføre ældre lovbestemmelser med samfundsudviklingen.[205] Kritikken af

---

[201] Toftegaard Nielsen: "*Strafferet I – Ansvaret*", 2013, s. 43 ff. Cfr. Vagn Greves retspolitiske synspunkter om dette princip, "in dubio mitius", i Vagn Greve: "Om hjemmelen for administrative straffebestemmelser", i "*Lov og Frihet Festskrift til Johs. Andenæs*" af Anders Bratholm, Nils Christie og Torkel Opsahl (red.), 1982, s. 124 f.

[202] Baumbach gennemgår retspraksis i "*Det strafferetlige legalitetsprincip – hjemmel og fortolkning*", 2008, s. 414 ff., og for så vidt nyere retspraksis se Baumbach: "Det strafferetlige legalitetsprincip - i straffeloven og i Menneskerettighedskonventionen – Om begrænset udvidende fortolkning og forudsigelighed", TfK 2013.105.

[203] Baumbach: "*Det strafferetlige legalitetsprincip*", 2008, s. 414, med henvisning til Gorm Toftegaard Nielsen: "*Strafferet I – Ansvaret*", 2004, s. 48 (se endvidere Toftegaard Nielsen: "*Strafferet I – Ansvaret*", 2013, s. 46 f.)

[204] Jf. referatet i Bet. 1417/2002, pkt. 2.6.

[205] Christina D. Tvarnø og Ruth Nielsen: "*Retskilder og retsteorier*", 2017, s. 230 f.

dommen går ifølge Tvarnø og Nielsen imidlertid på, at der ikke var årsagernes lighed, navnlig ved at der mangler ydre lighed mellem at bryde et brev og montere en lytteanordning, og når yderligere henses til, at der var tale om straf, er vurderingen, at dommen går for vidt i sin analogi-slutning og burde have overladt en sådan retsudvikling til lovgiver, der senere har reguleret telefonaflytning i straffeloven.[206]

I U 1990.70/2 H blev den tiltalte frifundet for dokumentfalsk i et tilfælde, hvor den pågældende havde benyttet en andens navn som underskrift på en telex. Landsretten fandt ikke, at telexansøgningerne kunne karakteriseres som et dokument i straffelovens forstand. Afgørelsen er fra før, straffelovens § 171 blev ændret til også at omfatte elektroniske dokumenter.[207]

I dommen, refereret i U 1996.356 Ø, havde den tiltalte deltaget i et system, hvor han modtog en diskette og for 50 kr. købte nogle koder, hvorefter det ville være muligt at kopiere programmet til videregivelse, således at senere led i kæden betalte 50 kr. 'tilbage' i kæden. Landsretten fandt, at det etablerede system var opbygget i samme form som kædebreve, og at formålet med at deltage i systemet var at opnå en økonomisk gevinst, og dermed måtte forholdet anses for omfattet af forbuddet mod indsamling ved kædebreve i indsamlingslovens § 2. Den omstændighed, at kommunikationen i et vist omfang skete ved anvendelse af disketter til pc'er, ses ikke at udelukke, at fremgangsmåden anses som kædebreve i lovens forstand.[208]

Brydensholt-udvalget tog i Betænkning 1417/2002, pkt. 2.6., stilling til, hvorvidt der på baggrund af udviklingen på IT-området var behov for at justere de strafferetlige regler. I tilknytning til analogiforbuddet i straffelovens § 1 og EMRK artikel 7, stk. 1, var det udvalgets vurdering, at danske domstole ikke havde ført nogen entydig praksis med hensyn til betydningen af analogiforbuddene i relation til nye teknologiske fænomener, og at det *"ikke var muligt at opstille nogen klar prognose om, hvorledes domstolene vil fortolke eksisterende straffebestemmelser i henseende til nye teknologiske fremtrædelsesformer, der ikke klart dækkes af de pågældende bestemmelsers ordlyd."*[209] Udvalget var opmærksom på, at man i videst muligt omfang måtte

---

[206] Christina D. Tvarnø og Ruth Nielsen: "*Retskilder og retsteorier*", 2017, s. 230 f., Bernhard Gomard: "Analogi i strafferetten" i "*Festskrift til Alf Ross*" af Mogens Blegvad, Max Sørensen, Isi Foighel, Jørgen Trolle og A. Vinding Kruse (red.), 1969, s. 131, Bernhard Gomard: "Den tekniske udvikling og retssystemet", U 1963B.205, s. 212, Mads Bryde Andersen: "*IT-retten*", 2005, s. 724, Stuer Lauridsen: *"Pressefrihed og personlighedsret"*, 1988, s. 187, samt Brydensholt-udvalgets Bet. 1417/2002, pkt. 2.6.

[207] Ændringen skete ved lov nr. 352 af 19. maj 2004.

[208] Om dommen, se Baumbach: "*Det strafferetlige legalitetsprincip*", 2008, s. 418 f., og Mads Bryde Andersen: "*IT-retten*", 2005, s. 724 f.

[209] Bet. 1417/2002, pkt. 2.6.

tilgodese både kravet om klar lovhjemmel og ønsket om en lovgivning, der var fremtidstilpasset til den teknologiske udvikling.[210]

3.2. Legalitetskrav og forudsigelighed, jf. EMRK artikel 7, stk. 1

Det følger af artikel 7, stk. 1, 1. pkt., at en gerning kun kan straffes, hvis den udgjorde en forbrydelse efter national eller international ret på det tidspunkt, da den blev begået.[211] Heri ligger som tidligere nævnt et legalitetskrav, hvor det særligt må bemærkes, at der ikke gives nogen mulighed for undtagelse fra artikel 7, ej heller i krigstid, jf. artikel 15.

Som tidligere nævnt, har EMD fastlagt et 'analogi-forbud' i relation til artikel 7, stk. 1, som i *Kokkinakis*-sagen blev formuleret således: "*It also embodies, more generally, the principle that only the law can define a crime and prescribe a penalty (nullum crimen, nulla poena sine lege) and the principle that the criminal law must not be extensively construed to an accused's detriment, for instance by analogy.*"[212]

Om rækkevidden af EMRK' analogiforbud sammenholdt med den danske straffelovs § 1, der tillader analogi til en vis grad, har Baumbach på baggrund af en analyse af EMD's praksis anført, at der er intet, der tyder på, at Domstolens forbud ville omfatte den danske fortolkningsvariant "fuldstændig lovanalogi."[213] Dette skyldes, at EMD i sin praksis tillader, at en bestemmelses anvendelsesområde ikke nødvendigvis er endeligt fastlagt på gerningstidspunktet, men må fortolkes og fastlægges fra sag til sag,

---

[210] Bet. 1417/2002, pkt. 2.6.

[211] Jf. princippet *Nullum crimen, nulla poena sine lega*, hvoraf følger: "only the law can define a crime and prescribe a penalty", jf. Rainey, Wicks and Ovey: "*The European Convention on Human Rights*", 7th edition, 2017, s. 328 ff. Se endvidere Baumbach: "*Det strafferetlige legalitetsprincip*", 2008, s. 233 ff. og 441 ff., Baumbach: "*Strafferet og menneskeret*", 2014, s. 127 ff., Kjølbro: "*Den Europæiske Menneskerettighedskonvention for praktikere*", 2017, s. 733 ff., Helena Lybæk Guðmundsdóttir: *"Clarifying broad hacking statutes"*, 2015, s. 76 ff., Harris, D.J., M. O'Boyle, E. Bates og C. Buckley: "*Law of European Convention on Human Rig*hts", 4th edition, 2018, s. 491 ff., samt Schabas, W.: "*The European Convention on Human Rights*", 2015, 329 ff.

[212] *Kokkinakis mod Grækenland,* dom af 25. maj 1993, pkt. 52. EMD's analogiforbud går længere tilbage, se eksempelvis de tidligere klagesager, *X. mod Østrig*, (1852/63) afgørelse af 22. april 1965, *X. mod Storbritannien*, (6683/74) afgørelse af 10. december 1975, og *X. mod Holland* (7721/76) afgørelse af 12. december 1977.

[213] Baumbach: "*Strafferet og menneskeret*", 2014, s. 81.

og at en sådan retsudvikling kan være lovlig og ikke stridende mod EMRK.[214] Baumbachs vurdering forekommer rigtig, med henvisning til praksis, der følger nærmere nedenfor.

I tilknytning til legalitetskravet i artikel 7, stk. 1, 1. pkt., har EMD fastlagt en række kvalitative krav til en straffebestemmelses gyldighed, hvilket inddrages i det følgende. Disse krav kan ses som forudsætning for forbuddet mod analogi/udvidet fortolkning, eller "to sider af samme sag". Som formuleret af Rainey, Wicks and Ovey: *"since the more precisely drafted an offence is, the less scope there is for creative judicial interpretation and nasty courtroom surprises for defendants."*[215]

I den engelske affattelse af EMRK er det danske ord "ret" angivet som "law", som dermed er det gennemgående begreb både i artikel 7 og i relation til artikel 8-11, hvor indgreb i frihedsrettighederne efter bestemmelsernes stk. 2 skal ske "in accordance with the law"/"prescribed by law", og EMD stiller samme kvalitative krav til retsgrundlaget: At der er tale om 'ret', men ikke nødvendigvis udtrykkelig lovgivning, men også uskreven ret, herunder retspraksis, og at det retlige grundlag skal være tilgængeligt for borgeren, og retstilstanden være forudsigelig.[216] Om denne forudsigelighed udtalte EMD i *Kokkinakis mod Grækenland*: *"…an offence must be clearly defined in law. This condition is satisfied where the individual can know from the wording of the relevant provision and, if need be, with the assistance of the courts' interpretation of it, what acts and omissions will make him liable*."[217]

EMD har i sin praksis efter artikel 7, stk. 1, 1. pkt., taget stilling til forskellige aspekter af denne 'forudsigelighed.' Således kan en retstilstand godt være forudsigelig for borgeren, selv om det er første gang, de nationale domstole nu skal tage stilling til

---

[214] Baumbach: "*Strafferet og menneskeret*", 2014, s. 81 og 141 f., se endvidere Harris, O'Boyle, Bates og Buckley: "*Law of European Convention on Human Rights*", 4th edition, 2018, s. 494 f., og Schabas: "*The European Convention on Human Rights*", 2015, s. 338 f.

[215] Rainey, Wicks and Ovey: "*The European Convention on Human Rights*", 7th edition, 2017, s. 328.

[216] *Cantoni mod Frankrig*, dom af 11. november 1996, pkt. 29, *Del Río Prada mod Spanien*, Storkammerets dom af 21. oktober 2013, pkt. 91, og *Navalnyye mod Rusland*, dom af 17. okt. 2017, pkt. 54. Se endvidere Baumbach: "*Strafferet og menneskeret*", 2014, s. 129 f. og 142 ff., Kjølbro: *"Den Europæiske Menneskerettighedskonvention for praktikere"*, 2017, s. 743, Harris, O'Boyle, Bates og Buckley: "*Law of European Convention on Human Rights*", 4th edition, 2018, s. 492 ff., samt Schabas: "*The European Convention on Human Rights*", 2015, s. 336 f. Se om legalitetskravet i tilknytning til artikel 8, stk. 2, Artikel 5: *"Politiets infiltration på digitale platforme – set i et menneskeretligt perspektiv*", pkt. 4.3.

[217] *Kokkinakis mod Grækenland*, pkt. 52-53.

et sådant forhold, og der således ikke er tidligere retspraksis, som borgeren kunne have orienteret sig i. Dette forudsætter ifølge EMD, at den retstilstand, som domstolene når frem til, kan siges at være *"both foreseeable and consistent with the essence of the offence."*[218]

Uanset udgangspunktet om at borgeren skal kunne forudsige, hvad der er strafbart, ses EMD dog i vidt omfang at acceptere straffebestemmelser med generelle begreber, der skal underlægges en fortolkning. Som EMD udtalte i *Kafkaris mod Cypern* fra 2008: "*The Court has acknowledged in its case-law that however clearly drafted a legal provision may be, in any system of law, including criminal law, there is an inevitable element of judicial interpretation. There will always be a need for elucidation of doubtful points and for adaptation to changing circumstances. Again, whilst certainty is highly desirable, it may bring in its train excessive rigidity and the law must be able to keep pace with changing circumstances. Accordingly, many laws are inevitably couched in terms which, to a greater or lesser extent, are vague and whose interpretation and application are questions of practice*."[219]

Endvidere har EMD udtalt, at artikel 7 ikke er udtryk for et forbud mod, at en retstilstand udvikler sig i takt med tiden, således at der sker "*gradual clarification of the rules of criminal liability through judicial interpretation from case to case, provided that the resultant development is consistent with the essence of the offence and could reasonably be foreseen*."[220]

En sådan gradvis retsudvikling var tilfældet i *Eurofinacom mod Frankrig*,[221] hvor en digital platform på det franske 'Minitel' blev dømt for at agere formidler mellem

---

[218] *Navalnyye mod Rusland*, dom 17. okt. 2017, pkt. 56, med henvisning til *Jorgic mod Tyskland,* dom af 12. juli 2007, pkt. 114, *Custers, Deveaux and Turk mod Danmark*, dom af 3 maj 2007, *Soros mod Frankrig*, dom af 6. oktober 2011, og *Huhtamäki mod Finland,* dom af 6. marts 2012, pkt. 51.

[219] Storkammerets dom af 12. februar 2008, pkt. 141. Se hertil Kjølbro: *"Den Europæiske Menneskerettighedskonvention for praktikere"*, 2017, s. 744 f., og Rainey, Wicks and Ovey: "*The European Convention on Human Rights*", 7th edition, 2017, s. 334.

[220] Se bl.a. *Streletz, Kessler and Krenz mod Tyskland*, Storkammerets dom af 22. marts 2001, pkt. 50, *Navalnyye mod Rusland*, dom af 17. oktober 2017, pkt. 55, *Del Río Prada mod Spanien*, Storkammerets dom af 21. oktober 2013, pkt. 93, *S.W. mod Storbritannien*, dom af 22. november 1995, pkt. 36; *K.-H. W. mod Tyskland*, Storkammerets dom af 22. marts 2001, pkt. 45, og *Rohlena mod Tjekkiet,* Storkammerets dom af 27. januar 2015, pkt. 50. Se endvidere Kjølbro: *"Den Europæiske Menneskerettighedskonvention for praktikere"*, 2017, s. 745, og Rainey, Wicks and Ovey: "*The European Convention on Human Rights*", 7th edition, 2017, s. 334.

[221] Klagesag af 7. september 2004, hvor EMD afviste at realitetsbehandle klagen.

prostituerede og deres kunder. Der var ikke under sagen for EMD fremlagt noget fransk retspraksis, der fastslog, at den form for passiv formidling af kontakt hidtil var fundet strafbar.[222] Men strafbarheden var efter EMD's opfattelse tilstrækkeligt forudsigelig, med henvisning til at artikel 7 ikke udelukker *"the gradual clarification of the rules of criminal liability through judicial interpretation from case to case, "provided that the resultant development is consistent with the essence of the offence and could reasonably be foreseen""*[223] ligesom EMD henviste til, at lovgivers hensigt tydeligvis havde været at straffe alle former for formidlingsaktivitet mellem prostituerede og deres kunder. Endvidere lagde EMD vægt på, at klageren som erhvervsdrivende virksomhed i kommunikations-sektoren, måtte udvise særlig omhu med at orientere sig i retsgrundlaget.

Dommen i *Eurofinacom mod Frankrig* kan ses som eksempel på, at en straffebestemmelse, der har sin oprindelse i en analog kontekst, stadig kan indebære en forudsigelig retstilstand, når den anvendes i en ny og digital kontekst. Formidlingen og kontaktfladen har ændret karakter, men essensen af forbrydelsen er den samme. I samme retning ses *Isaksson og andre mod Sverige*, om ulovligt salg på internettet af narkotika og medicin, hvor EMD afviste at realitetsbehandle klagen.[224]

I både *Eurofinacom mod Frankrig* og *Kokkinakis mod Grækenland* var det strafbare forhold beskrevet i forholdsvis brede begreber, uden at dette medførte krænkelse af artikel 7, stk. 1.

Den centrale dom for så vidt angår brede straffebestemmelser, er *Cantoni mod Frankrig.*[225] Klageren var indehaver af et supermarked, der havde solgt forskellige produkter, som var omfattet af en bredt formuleret regulering af "medicinske produkter", som var forbeholdt salg via apotek. Han gjorde gældende, at det retlige grundlag for at idømme straf ikke var tilstrækkeligt præcist. EMD fandt ikke, at der var sket en krænkelse af artikel 7, stk. 1 og udtalte blandt andet: *"Like many statutory definitions, that of "medicinal product" contained in Article L. 511 of the Public Health Code is rather general (---). When the legislative technique of categorisation is used, there will often be grey areas at the fringes of the definition. This penumbra of doubt in relation to borderline facts does not in itself make a provision incompatible with Article 7 (art. 7), provided that it proves to be sufficiently clear in the large majority of cases. The role of adjudication vested in the courts is precisely to dissipate such interpretational doubts as remain, taking into account the changes in everyday*

---

[222] *Eurofinacom mod Frankrig*, se hertil Kjølbro: *"Den Europæiske Menneskerettighedskonvention for praktikere"*, 2017, s. 747.
[223] Med henvisning til *Streletz, Kessler and Krenz mod Tyskland*, Storkammerets dom af 22. marts 2001, pkt. 50.
[224] *Isaksson og andre mod Sverige,* afgørelse af 8. marts 2016.
[225] Storkammerets dom af 11. november 1996.

practice. The Court must accordingly ascertain whether in the present case the text of the statutory rule read in the light of the accompanying interpretive case-law satisfied this test at the relevant time."[226]

I *Cantoni*-sagen lagde EMD vægt på, at om end der var divergerende retspraksis, afsagt i andre sager i førsteinstansen, havde ankeinstansen altid anlagt en udvidet fortolkning og således *"never upheld a decision by a lower court finding that such a product fell outside the notion of medicinal product."*[227] Ligeledes lagde EMD vægt på, at en retstilstand er forudsigelig, selv om borgeren må antage juridisk bistand for at kunne vurdere *"to a degree that is reasonable in the circumstances, the consequences which a given action may entail"*, hvilket så meget desto mere gælder, når der var tale om erhvervsmæssig virksomhed, og derved var det forudsigeligt for klageren, at han *"ran a real risk of prosecution for unlawful sale of medicinal products."*[228]

Cian C. Murphy har i sin analyse af EMD-praksis om forudsigelighed i tilknytning til EMRK artikel 7 inddraget et princip, *"The 'thin ice' principle", som er anvendt af Lord Morris i en engelsk straffesag til at beskrive den situation, at "those who skate on thin ice can hardly expect to find a sign which will denote the precise spot where he [sic] will fall in."*[229] Princippet indebærer, at en gerningsmand, der vidste, at han bevægede sig ud i gråzonen af et strafbart område, selv bærer risikoen for den strafforfølgning, der kan blive konsekvensen. Murphys synspunkt er, at når EMD i sine

[226] Pkt. 32. Denne formulering af forudsigelighed i forhold til "the large majority of cases", er siden gentaget af Domstolen i *Soros mod Frankrig*, dom af 6. oktober 2011, pkt. 52. I senere domme henvises i vidt omfang til den næste sætning i *Cantoni mod Frankrig*, pkt. 32, om "*the role of adjudication",* se eksempelvis *Del Río Prada mod Spanien*, Storkammerets dom af 21. oktober 2013, pkt. 93.

[227] Pkt. 34.

[228] Pkt. 35. I samme retning om at antage juridisk bistand, *Groppera Radio AG mod Schweiz,* dom af 28. marts 1990, pkt. 68.

[229] Cian C. Murphy: "The Principle of Legality in Criminal Law under ECHR", (November 16, 2009) i European Human Rights Law Review, Vol. 2, 2010, s. 192, hvor der henvises til sagen Knuller v DPP [1973] AC 435, i Andrew Ashworth: *"Principles of Criminal Law"* (Oxford) OUP 2009, s. 63 et seq. Sagen er tillige behandlet i den nye udgave, Jeremy Horder: *"Ashworths's Principles of Criminal Law*", 9th Edition, 2019, s. 86. Knuller-sagen omhandlede et tidsskrift, som optog annoncer, der inviterede til "homosexual practices", og dommen mod de ansvarshavende angik "conspiracy to corrupt public morals and conspiracy to outrage public decency."

afgørelser henviser til, at klageren må indse, at der er en risiko for strafferetlige sanktioner, er dette egentlig i modstrid med kravet om forudsigelighed i artikel 7.[230]

Helena Lybæk Guðmundsdóttir har i sin ph.d.-afhandling "Clarifying Broad Hacking Statutes", Aalborg Universitet, 2015, foretaget en analyse af den danske og amerikanske 'hacking'-bestemmelse, og som led heri bl.a. inddraget EMRK artikel 7. I relation til forudsigelighed er Guðmundsdóttir ganske kritisk over for the 'thin ice' principle: "*Furthermore, if the only thing that is foreseeable is that the statute enables or encourages arbitrary enforcement or unforeseeable enforcement; that which is foreseeable is merely the ever-looming possibility of prosecution for any and all conduct related to e.g. computers, then there is equally little protection from arbitrary use of power as if there had been no pre-existing law. A thin ice principle is thus a rather unsettling idea, because even a statute prohibiting "any conduct that offends the state in any way" technically provides foreseeability in the sense that one must always tread carefully with respect to the state, the thin ice principle neglects even the most serious risks of arbitrary enforcement, placing the risk of prosecution on the basis of an unclear statute with a defendant. Furthermore, the principles seems to invite the notion that if there is uncertainty about the criminality of the defendant's conduct there ought to be a presumption of criminality, rather than requiring the legislature to speak in a more concise manner. In other words, the principle also seemingly invites the possibility of extensive construction and analogy (because the thin ice looms in the penumbra and with analogous behaviour), both of which are ostensibly precluded by article 7 ECHR*."[231]

Af EMD's praksis synes at kunne udledes, at der skal ganske meget til, før et retsgrundlag er for bredt formuleret til, at borgeren kan forudsige sin retstilstand, og de sager, hvor EMD har statueret krænkelse af artikel 7, stk. 1 angår mere håndgribelige juridiske betænkeligheder. Til eksempel *Dragotoniu og Militaru-Pidhorni mod Rumænien,*[232] hvor to personer, der var ansat i en privat bank, var tiltalt for at have taget imod bestikkelse ved overtrædelse af straffebestemmelse, der efter sin ordlyd alene angik offentligt ansatte, og der forelå ikke retspraksis, hvor bestemmelsen var anvendt på ansatte i private virksomheder.[233]

---

[230] Cian C. Murphy: "The Principle of Legality in Criminal Law under ECHR", med henvisning til *Coëme og andre mod Belgium*, dom af , 22. juni 2000, pkt. 150, og *Custers, Deveaux og Turk mod Danmark*, dom af 3. maj 2007, pkt. 81.

[231] Guðmundsdóttir: *"Clarifying broad hacking statutes"*, 2015, s. 100.

[232] Dom af 24. maj 2007, se hertil Schabas: "*The European Convention on Human Rights*", 2015, s. 335.

[233] Pkt. 42-43. Værd at bemærke er dommens pkt. 40, hvor EMD understregede kravet om en strikt fortolkning af straffebestemmelser: "*Comme corollaire du principe de la légalité des condamnations, les dispositions de droit pénal sont soumises au*

Som et sjældent eksempel på, at EMD har statueret krænkelse af artikel 7, stk. 1 som følge af en for bred formulering og vage begreber, kan fremhæves *Liivik mod Estland* fra 2009,[234] hvor klageren var direktør i en offentlig enhed, der skulle gennemføre privatisering af et statsligt jernbaneselskab. EMD understregede, at det først og fremmest var et anliggende for de nationale myndigheder, herunder navnlig domstole, at fortolke national ret, og at EMD's rolle var begrænset til at fastslå, om resultatet af en sådan fortolkning er forenelig med EMRK.[235] Som EMD påpegede, var der i sagen tale om en straffebestemmelse som hidrørte fra det tidligere sovjetiske retssystem, og som nu skulle anvendes i en helt ny kontekst af markedsøkonomi, og straffesagen mod klageren angik "*creating a situation whereby the preservation of the State's assets might have been jeopardised and that this was considered significant damage despite the fact that the risks had not materialized*." Derudover var han fundet skyldig i at have *"caused significant moral damage to the interests of the State – as the Court of Appeal put it, the applicant's acts had not been in compliance with "the general sense of justice."*[236] Konklusionen var, at EMD "*finds on the whole that the interpretation and application of Article 161 in the present case involved the use of such broad notions and such vague criteria that the criminal provision in question was not of the quality required under the Convention in terms of its clarity and the foreseeability of its effects*."[237]

Sammenfattende kan det konstateres, at EMRK artikel 7' s krav om forudsigelighed indeholder en række, analytiske elementer udviklet gennem EMD's retspraksis siden *Kokkinakis*-dommen. Som påpeget af Guðmundsdóttir, adskiller artikel 7 sig fra den vurdering, EMD skal foretage efter artikel 8-11, når der skal gøres indgreb i frihedsrettighederne, og hvor EMD ud over det retlige grundlag også skal inddrage de legale hensyn bag og nødvendigheden af indgrebet (proportionalitet).[238] Den vurdering, EMD foretager efter artikel 7, forekommer derfor at være af mere snæver, juridisk,

---

principe d'interprétation stricte." Se om dommen, Kjølbro: *"Den Europæiske Menneskerettighedskonvention for praktikere"*, 2017, s. 749 f.

[234] Dom af 25. juni 2009, pkt. 94-104, se hertil Kjølbro: *"Den Europæiske Menneskerettighedskonvention for praktikere"*, 2017, s. 748, samt Guðmundsdóttir: *"Clarifying broad hacking statutes"*, 2015, s. 87 f.

[235] Pkt. 95. Se om dette tillige *Del Río Prada mod Spanien*, Storkammerets dom af 21. oktober 2013, pkt. 57, hvor EMD udtalte: *"according to its general approach, the Court does not question the interpretation and application of national law by national courts unless there has been a flagrant non-observance or arbitrariness in the application of that law.*"

[236] Pkt. 97-98.

[237] Pkt. 101.

[238] Guðmundsdóttir: *"Clarifying broad hacking statutes"*, s. 102 f.

teknisk karakter, og EMD skal som udgangspunkt ikke vurdere baggrunden for kriminaliseringen eller proportionaliteten heri. Uagtet denne juridisk-analytiske tilgang, må man ikke glemme, at vurderingen, der skal foretages efter artikel 7, er udtryk for to væsentlige og modstridende hensyn: på den ene side hensynet til borgeren og dennes retssikkerhed, og på den anden side hensynet til at de enkelte lande kan udvikle, graduere og modernisere egne straffebestemmelser i lyset af bl.a. den teknologiske udvikling, samtidig med at de enkelte lands særlige retstraditioner, særlig vægt på retspraksis, forarbejder eller andet, respekteres. Som på andre områder af EMRK anlægges formentlig også her af EMD en form for 'margin of appreciation', således at kun grovere tilfælde eller mere udtrykkelige juriske fejlkonstruktioner medfører en krænkelse af artikel 7. Guðmundsdóttirs kritik er dog berettiget, da brede, nationale straffebestemmelser generelt udfordrer forudsigeligheden, som er helt central for beskyttelsen efter artikel 7. Måske på sigt, i takt med at EMD's retspraksis på dette område bliver mere omfattende, og de retlige standarder udvikles og raffineres, vil vi opleve, at EMD går mere restriktivt og dynamisk til værks ved vurderingen af meget brede og vage straffebestemmelser.

Selv om retssikkerheden for den enkelte bedst tilgodeses ved klarhed og forudsigelighed i retstilstanden, er der lovgivningsteknisk tale om en balancegang, hvori tillige må indgå, at lovgivningen ikke bliver for kausistisk præget. Som Knud Waaben formulerede det i 1994, *"er det forkert at tro at brugen af straffebud med ubestemte og vurderingsprægede elementer, almenbegreber etc. er noget som man gradvis kan komme bort fra. Denne lovteknik er en pris som har måttet betales for at overvinde den kasuistiske skrivemåde der efterlader huller i loven."*[239]

4. 'Hacking'-bestemmelsen i lyset af legalitetsprincippet

Spørgsmålet er, hvordan den danske 'hacking'-bestemmelse i straffelovens § 263, stk. 1 stiller sig i forhold til det strafferetlige legalitetsprincip i straffelovens § 1 og i EMRK artikel 7, stk. 1.

Der er ingen tvivl om, at gerningsindholdet i straffelovens § 263, stk. 1 består af meget brede begreber, "uberettiget", "adgang" og "datasystemer"/"informationssystemer", hvor retspraksis har givet bestemmelsen et meget bredt indhold ved at fastslå, at bestemmelsen også finder anvendelse på de digitale platforme, jf. U 2015.345 Ø (Skattemappe-sagen) og U 2017.247 V (Ekskærestens Facebook-sagen). Der har ikke i lovforarbejder eller andet været formuleret nogen indskrænkelser i bestemmelsen, der kunne støtte en opfattelse af, at uberettiget adgang på rene digitale platforme, ikke var omfattet af bestemmelsens anvendelsesområde. Særligt i relation til 'hacking'-bestemmelsens gerningsindhold, "uberettiget adgang", vil der til stadighed i en digital kontekst udvikles nye måder at opnå adgang på, hvor domstolene må fortolke

[239] Knud Waaben: "Lovkravet i strafferetten", Nordisk Tidsskrift for Kriminalvidenskab, 1994, s. 131.

og fastlægge nye scenarier i forhold til straffebestemmelsens anvendelsesområde, f.eks. når velmenende IT-'hackere' tester systemer. Således er straffelovens § 263, stk. 1 udtryk for en straffebestemmelse, hvor en løbende, teknologisk fortolkning og gradvis udvikling vil være forventelig og i vidt omfang vil blive accepteret.

Den danske 'hacking'-bestemmelse vil derfor formentlig ikke være i strid med analogiforbuddet i straffelovens § 1 og EMRK artikel 7, stk. 1, hvilket støttes af, at bestemmelsen er udformet i overensstemmelse med Cybercrimekonventionens artikel 2, og således både er i overensstemmelse med Europarådets egne anbefalinger til kriminaliseringen og dertil også er sammenlignelig med en række andre landes kriminalisering.

Dog med forbehold for de nye og mere svigagtige digitale scenarier, som beskrevet i Artikel 1: *"'Hacking' og det digitale privatliv"*, eksempelvis som i den amerikanske *Drew*-sag, hvor det er overtrædelse af en række, ensidigt fastsatte og vagt formulerede kontraktsvilkår, der kommer til at danne grundlag for en straffesag om uberettiget adgang til et datasystem. Som også den amerikanske dommer i *Drew*-sagen nåede frem til, er det i høj grad tvivlsomt, om strafansvaret er forudsigeligt ved overtrædelsen af sådanne kommercielle kontraktsvilkår, dette navnlig henset til den almindelige internetadfærd, hvor ikke alle brugere i alle sammenhænge er helt sandfærdige om egne oplysninger. Ligeledes henset til, at serviceudbydere i almindelighed ikke politianmelder sådanne overtrædelser af kontraktsvilkår, og brugerne heller ikke forventer, at dette sker.

Uanset hvordan udfaldet måtte blive af sådanne situationer omsat til en konkret dansk straffesag, sammenholdt med straffelovens § 1 og EMRK artikel 7, må det erindres, at formålet med straffelovens regulering ikke er, at få så mange borgere straffet som muligt, men derimod helt grundlæggende at fastsætte forudsigelige rammer for det strafbare område, som borgerne kan indrette sig i tillid til. Når der allerede nu kan ses problemer i 'hacking'-bestemmelsens anvendelsesområde, og flere nye problematikker kan forudsiges i forhold til de sociale medier, er der en anledning til at genoverveje ordlyden og kriminaliseringen, for at tage stilling til hvor grænserne for det strafbare område skal gå.

5. Retspolitiske betragtninger

Det må overvejes, hvordan 'hacking'-bestemmelsen bedst afbalancerer de to hensyn over for hinanden, hensynet til at den enkelte kan beskytte sine data og systemer mod uberettiget adgang over for den frihed, der generelt præger internettet og som sikrer, at vi kan søge viden, kommunikere og måske endda drille hinanden uden at risikere strafansvar, jf. Artikel 1: *"'Hacking' og det digitale privatliv"*, pkt. 1.

Navnlig scenariet med de sociale medier synes at nødvendiggøre en indsnævring af 'hacking'-bestemmelsens anvendelsesområde, hvilket kunne gøres ved at indarbejde kravet fra Cybercrimedirektivet om, at en sikkerhedsforanstaltning skal være brudt. Derved kunne sikres, at ejeren af data og system selv har gjort det fornødne for at sikre sit datasystem og sine private oplysninger, før et strafansvar kommer på tale. Ved et krav om, at en sikkerhedsforanstaltning skal være brudt, undgås situationer, hvor det bliver en straffesag, at ekskæresten får adgang til Facebook-profilen for at drille, når forurettede selv har givet hende password og undladt at ændre password efter kæresteforholdets ophør. Konsekvensen er tillige, at sager som Facerape ej heller bliver til straffesager. I sådanne sager, hvor forurettede har undladt at sikre sine data og systemer, må man overveje at søge krænkelsen godtgjort civilretligt. Man vil altså ikke være 'hacker' i straffelovens forstand. Hvad der teknisk skal kræves, for at der er tale om en sikkerhedsforanstaltning, er et spørgsmål, der må afklares i retspraksis i lyset af den teknologiske udvikling.[240] En fordel ved en sådan ændret kriminalisering ville også være, at den danske bestemmelse bringes i overensstemmelse med de øvrige EU-landes kriminalisering.

Ved en sammenligning til den fysiske verden kan det konstateres, at det er strafbart at skaffe sig uberettiget adgang til andres boliger, selv om døren er ulåst, jf. straffelovens § 264, stk. 1, nr. 1. Desuden følger det af bestemmelsens nr. 2, at det er strafbart at undlade at forlade fremmed grund efter at være opfordret dertil. Det er fristende at forsøge at allegorisere fra den strafferetlige regulering af disse fysiske rammer til at udvikle tilsvarende normer til de digitale platforme, men øvelsen er svær. I den fysiske verden er de kulturelle normer om adgang til andres boliger og steder indarbejdet gennem adskillige år, og den strafferetlige regulering understøtter disse normer, mens den digitale kultur endnu ikke i nær samme grad er etableret.[241] Internettet er som udgangspunkt en offentlig tilgængelig platform, og der gives ikke noget entydigt svar på en række af de parametre, der indgår i § 264: Hvor går de virtuelle havelåger, indgangsdøre, kan man lægge nøgler under måtten, hvordan råber man hinanden an om at forlade fremmed grund, med en strafferetlig konsekvens af at forblive på stedet. Uanset dette forsøg på at overføre fysiske normer til digitale normer, vil spørgsmålet alligevel være, om der nødvendigvis skal være en overensstemmelse mellem den fysiske og den digitale verden, hvis saglige hensyn taler for at anlægge visse forudsætninger for strafansvaret i relation til 'hacking'-bestemmelsen i straffelovens § 263, stk. 1.

Såfremt brud på en sikkerhedsforanstaltning bliver en forudsætning for strafansvar, kan man dog forestille sig helt særlige situationer, hvor dette krav ville forekomme

[240] Jf. Artikel 1: *"'Hacking' og det digitale privatliv",* pkt. 4.

[241] Jf. Artikel 1: *"'Hacking' og det digitale privatliv",* pkt. 5.4*.,* med henvisning til Guðmundsdóttir: *"Clarifying broad hacking statutes"*, 2015, s. 238, og Orin S. Kerr: "Norms of computer trespass (essay)", Colombia Law Review, 1143 (2016).

for rigidt, og hvor den onde vilje har for frit spil. Man kan f.eks. forestille sig, at professionelle 'hackere' bryder en sikkerhedsforanstaltning på et system, f.eks. en netbank, hvor systemet efterlades åbent og uden sikkerhedsforanstaltning, hvorved andre personer får mulighed for en uhindret, uberettiget adgang. I sådanne tilfælde er det oplagt, at der sædvanligvis ville være en sikkerhedsforanstaltning, der nu grundet ekstraordinære omstændigheder er blevet brudt, og andre brugere kan derfor ikke skaffe sig berettiget adgang, hvilket man godt er klar over.

Et forsigtigt bud på en ændring af gerningsindholdet i 'hacking'-bestemmelsen, kunne være, at "man har skaffet sig uberettiget adgang til andres data i et datasystem, når adgangen er sket ved brud på en sikkerhedsforanstaltning eller på lignende indgribende måde." Herved gøres bruddet på en sikkerhedsforanstaltning til den absolutte hovedregel, dog vil der også være mulighed for strafansvar i andre lignende, ekstraordinære situationer. En sådan tilføjelse er dog ikke uproblematisk, både fordi den er vagt formuleret, og fordi der også her risikeres et vidt anvendelsesområde: ret beset kan en mobiltelefon, der endnu ikke har aktiveret sin skærmlås, siges normalt at være beskyttet ved en sikkerhedsforanstaltning, og dette er gerningsmanden klar over.[242] Den foreslåede formulering har væsentlig lighed med den norske 'hacking'bestemmelse i straffelovens § 204, der angår 'innbrud i datasystem', og hvor man straffes for *"å bryte en beskyttelse eller ved annen uberettiget fremgangsmåte skaffer sig tilgang til datasystem eller del av det."*[243] Til en inspiration til de danske overvejelser om en ændret kriminalisering i straffelovens § 263 kunne det være relevant nærmere at undersøge den norske kriminalisering og afdække erfaringerne hermed. Dette falder imidlertid uden for denne afhandlings rammer.

I relation til de sociale medier må lovgiver tage stilling til de svigagtige tilfælde, dvs. hvor adgangen sker efter en menneskelig validering ud fra nogle subjektivt fastsatte kriterier af administratoren af den konkrete profil, gruppe, 'zone' mv. Her må træffes et valg, om man fra lovgivers side mener, det skal kunne udløse et strafansvar, at man får adgang til interessegrupper mv. ved at have oplyst falske generalier, interesser, værdier mv. Eller om man som bruger af disse platforme, hvor man allerede ved oprettelsen af sin profil typisk har givet sit samtykke til, at platformen generelt kan overvåge og videregive oplysninger i bred forstand til en ubestemt kreds af annoncører og samarbejdsparter, også selv må løbe en risiko for, hvem man præcis interagerer med, i vished om, at ikke alle er, hvad de giver sig ud for at være. Den internetkutyme, som blev beskrevet i *Drew*-sagen, må man realistisk set forholde sig til, navnlig når der er tale om platforme, hvor identiteter mv. ikke valideres ud fra

[242] Jf. Inger Marie Sunde: "Cybercrime Law" i *"Digital Forensics"* af André Årnes (ed.), 2018, s. 85. Se endvidere om forskellige tilgange til en 'hacking'-bestemmelses kriminalisering, Guðmundsdóttir: *"Clarifying broad hacking statutes"*, 2015, navnlig konklusionen, s. 321 ff.

[243] Jf. hertil Inger Marie Sunde: *"Datakriminalitet"*, 2016, s. 63 ff.

Nem-id eller lignende, og hvor der omvendt er andre fordele forbundet ved, at der faktisk er mulighed for, at man kan debattere og afprøve synspunkter uden at fremstå i sit eget navn.

Det følger af straffelovens § 1, at straf kun kan pålægges for et forhold, hvis strafbarhed er hjemlet ved lov, eller som ganske må ligestilles med et sådant. Dette strafferetlige legalitetsprincip forudsætter, at det er beskrevet og forudsigeligt for borgeren, hvad der er strafbart, jf. også EMRK artikel 7, stk. 1. I den situation, hvor man skaffer sig uberettiget adgang til en gruppe ved svigagtigt at foregive at opfylde nogle mere eller mindre, flydende, subjektive kriterier, som administratoren har fastsat for at tillade adgang, ville dette være et meget løst og ubestemt grundlag at basere et strafansvar på, som også den amerikanske dommer vurderede i *Drew*-sagen. Mest synes at tale for at undtage sådanne situationer fra 'hacking'-bestemmelsens anvendelsesområde.[244]

6. Betydning for politiets 'hacking'

Den vanskelighed, som borgeren har med at forudsige, hvor præcist grænserne går mellem offentligt og privat område på internettet, gør sig ligeledes gældende for politiet, der kan have meget vanskeligt ved at vurdere, hvad der er offentligt tilgængeligt, og hvad der er privat område, hvortil adgangen udgør et tvangsindgreb, der kræver lovhjemmel. De to typesituationer udvalgt i artiklen om 'hacking' – IT-'hackeren' og 'hacking' på de sociale medier – er også metoder, som politiet kan anvende.

Den IT-'hacker', der undersøger systemet, kunne i stedet være en politimand, der undersøger systemet. Den skillelinje, som 'hacking'-bestemmelsen fastlægger for, hvor tæt på et datasystem man må gå – om man må undersøge specifikationer, teste osv. – kan også have en betydning for politiets adgang til systemet og vurderingen af, hvornår politiet kan siges at bevæge sig ind i borgerens privatliv. Spørgsmålet er, om politiet kan afprøve sikkerhed i videre omfang end borgeren. Her kan man måske forestille sig en gråzone, hvor borgeren vil blive straffet for forsøg på at få adgang, hvis forsættet netop er til at få adgang, men hvor politiet har et spillerum til at undersøge sikkerhedsforanstaltningerne – uden at have til hensigt til at få adgang – for at vurdere egen tekniske kapacitet, før der indhentes en retskendelse til indgrebet. Det er vel for så vidt ikke et indgreb mod privatlivet, hvis politiet fra den offentlige side undersøger systemet, så længe der ikke bruges teknologi til at få adgang til noget, man ellers ikke ville have haft adgang til, og der ikke ændres i systemets tekniske indstillinger. Således vil politiets undersøgelse og konstatering af, at X informationssystem beskyttes af Y foranstaltning, næppe kvalificere til et indgreb i privatlivet. Dog bortset fra det indgreb, der kan ligge i indsamling og behandling af offentligt tilgængelige oplysninger, jf. politilovens § 2 a, stk. 2, og EMRK artikel 8, stk. 2.

[244] I overensstemmelse med Guðmundsdóttirs vurdering af *Drew*-sagen i en amerikansk kontekst, *"Clarifying broad hacking statutes"*, 2015, s. 231 f.

I forhold til de sociale medier, kunne politiet også være interesserede i at få adgang til brugerkonti eller til lukkede grupper, hvilket ville give politiet mulighed for at overvåge deltagerne og kommunikationen imellem dem. Sådanne lukkede grupper kunne eksempelvis være handelspladser for euforiserende stoffer mv.[245] Her har administrator den fordel at skulle godkende adgang for nye medlemmer, ligesom alle i gruppen kan holde sig anonyme, og dertil kommer, at gruppen let kan lukkes ned, hvis man fornemmer, at myndighederne har fået kendskab til siden. Politiets adgang til sådanne grupper vil kunne forekomme som en teknisk 'hacking', men vil oftere ske ved, at politiet får adgang ved at skjule politiidentiteten og angive urigtige oplysninger.

Netop ved en sådan 'svigagtig' adgang skilles paralleliteten mellem borgerens strafansvar og politiets efterforskning, der kræver lovhjemmel. En svigagtig adgang vil for borgeren som udgangspunkt være strafbar 'hacking' ligeså vel som den tekniske 'hacking'. Derimod vil den 'svigagtige' adgang for politiet ikke indebære et strafprocessuelt tvangsindgreb, som den tekniske 'hacking' ellers ville gøre. Det skyldes, at den 'svigagtige' adgang for politiet rummes i den efterforskningsmetode, der betegnes som infiltration, jf. Artikel 4: *"Politiets hjemmel til 'hacking' som led i en efterforskning"* og Artikel 5*: "Politiets infiltration på digitale platforme – set i et menneskeretligt perspektiv."*

[245] Eksempelvis dokumenterede TV2' Kriminalmagasin, Station 2, i februar 2018 hvordan der fra grupper på Facebook blev solgt euforiserende stoffer, se link http://nyheder.tv2.dk/krimi/2018-02-28-det-flyder-med-narko-paa-facebook.

Kapitel 3 Reguleringen af politiets tekniske indgreb på internettet

1. Sammenfattende om retsplejelovens tekniske indgreb

Hjemlen til politiets tekniske indgreb for at skaffe sig adgang til borgerens private data, kan findes i tre forskellige reguleringer i retsplejeloven: Ransagningsreglerne, dataaflæsning og indgreb i meddelelseshemmeligheden. Disse tre regelsæt er behandlet i den tidligere artikel: "Hemmelig ransagning og brevstandsning i den digitale virkelighed",[246] samt denne afhandlings Artikel 3: "*Retsplejelovens regulering af politiets adgang til teledata*" og Artikel 4: "*Politiets hjemmel til 'hacking' som led i en efterforskning.*" I det følgende sammenfattes retstilstanden på baggrund af disse tre artikler.

Som anført i Artikel 4: "*Politiets hjemmel til 'hacking' som led i en efterforskning*" udgør ransagningsreglerne den almindelige hjemmel, når politiet ønsker at skaffe sig adgang til et privat/beskyttet datasystem, og i de tilfælde hvor adgangen sker hemmeligt, finder retsplejelovens § 799 om hemmelig ransagning anvendelse. Reglerne om dataaflæsning er anvendelige i de situationer, hvor politiet installerer et spionprogram, som fortløbende sender information om aktiviteten til politiet. Endelig dækker reglerne om indgreb i meddelelseshemmeligheden den situation, hvor politiet gør indgreb i en meddelelse, der er undervejs i en kommunikationslinie, under forudsætning af, at en teleudbyder eller anden udbyder bistår hermed.

Anvendelsesområdet for hver af disse tre regelsæt kendetegnes således af hvilken *metode*, politiet bruger til at få hemmelig adgang, hvorimod det som udgangspunkt uden betydning for adgangsreguleringen, hvad præcist det er for et *indhold*, som politiet forventer at finde inde i det beskyttede system, om det er en form for datalager, eller om det er kommunikation. Hvis politiet med egne 'hacking'-metoder kan skaffe sig adgang til en digital kommunikationsplatform, bringes indgrebet ikke ind under reglerne om indgreb i meddelelseshemmeligheden, uagtet politiet skaffer sig indsigt i en kommunikation i realtid, og derved kan siges at gøre indgreb i meddelelser "der er undervejs i en kommunikationslinie."

Alle tre regelsæt er restriktivt reguleret, både i forhold til de materielle betingelser og de processuelle krav, dog er reglerne om hemmelig ransagning i retsplejelovens

[246] Lene Wacher Lentz: "Hemmelig ransagning og brevstandsning i den digitale virkelighed", Juristen, 1/2016.

§ 799 begrænset til kun at finde anvendelse ved ganske få særligt nævnte forbrydelser, hvorimod reglerne om dataaflæsning og indgreb i meddelelseshemmeligheden som udgangspunkt kræver 6 års fængsel i strafferammen.[247]

Kort må her bemærkes, at Cybercrimekonventionen i artikel 14-21 indeholder en række proceduremæssige forpligtelser, blandt andet artikel 19, hvorefter staterne skal fastsætte regler, der giver mulighed for, at myndighederne kan ransage eller på lignende måde skaffe sig adgang til et edb-system mv.[248] Denne bestemmelse forekommer bredt formuleret, og det var også Justitsministeriets opfattelse i forbindelse med Konventionens gennemførelse, at denne konventionsforpligtelse var opfyldt med retsplejelovens ransagningsregler.[249] Spørgsmålet forfølges ikke yderligere her.

I det følgende inddrages et menneskeretligt perspektiv på den danske retstilstand, hvor tre regelsæt regulerer politiets adgang til datasystemer.

2. EMRK artikel 8, stk. 2

For de straffeprocessuelle tvangsindgreb, der er behandlet i denne afhandling – hemmelig ransagning, dataaflæsning og indgreb i meddelelseshemmeligheden – gælder, at sådanne indgreb i privatliv, korrespondance mv. skal opfylde kravene i EMRK artikel 8, stk. 2. Heraf følger, at indgreb kun må ske i overensstemmelse med loven, og såfremt indgrebet er nødvendigt i et demokratisk samfund af hensyn til de nærmere opregnede formål, herunder at forebygge uro eller forbrydelse.

Særligt i forhold til artikel 8 og de straffeprocessuelle tvangsindgreb, er det afgørende, om de relevante regler angiver, under hvilke betingelser indgrebet må finde sted, og om reglerne indeholder garantier mod vilkårlighed.[250] I forhold til indgreb i meddelelseshemmeligheden følger det af retspraksis, at nationale retsregler skal fastsætte en afgrænsning af de personer, der kan risikere at blive udsat for et tvangsindgreb, en angivelse af karakteren af den kriminalitet, der kan begrunde et indgreb, en tidsmæssig begrænsning af indgrebet, en procedure, hvorefter der skal foretages optegnelser over indgrebet og hvorved indholdet af resultatet fremgår, således at

[247] Lene Wacher Lentz: "Hemmelig ransagning og brevstandsning i den digitale virkelighed", Juristen, 1/2016, pkt. 4.5.
[248] Konventionen er gengivet i pkt. 7 i lovforslag nr. 55 af 5. november 2003.
[249] Lovforslag nr. 55 af 5. november 2003, pkt. 7.2, om Justitsministeriets overvejelser om lovgivningsmæssige konsekvenser, Del 2, processuelle bestemmelser. Se endvidere om Cybercrimekonventionens processuelle del, Inger Marie Sunde: "Cybercrime Law" i "*Digital Forensics*", André Årnes (red.), 2018, s. 95 ff.
[250] Se hertil *Camenzind mod Schweiz*, dom af 16. december 1997, pkt. 45, og Kjølbro: *"Den Europæiske Menneskerettighedskonvention for praktikere"*, 2017, s. 762.

dette kan kontrolleres af domstolene og forsvareren, foruden bestemmelser om destruktion, herunder navnlig i tilfælde, hvor den mistænkte efterfølgende frifindes.[251]

Legalitetskravets indhold afhænger af karakteren og intensiteten af indgrebet, og således følger det af retspraksis, at kravet til hjemmelsgrundlaget skærpes, når der er tale om alvorlige indgreb, såsom ransagning og beslaglæggelse,[252] og når der er tale om hemmelige indgreb, herunder indgreb i meddelelseshemmeligheden, hvor risikoen for misbrug fra myndighedernes side er større.[253] Dog har EMD udtrykt, at der i forhold til reguleringen af skjulte indgreb, såsom aflytning af telefoner, kan lovhjemlen ikke være så detaljeret, at personen kan siges at have mulighed for at indrette sin adfærd efter det.[254]

I relation til de mindre intensive indgreb har EMD eksempelvis fastslået, at politiet uden udtrykkelig hjemmel kan indsamle og optage beviser i forbindelse med en efterforskning, idet en sådan bemyndigelse må anses for forudsat, men at der kræves mere udtrykkelig hjemmel til at foretage mere indgribende foranstaltninger, såsom ransagning eller personundersøgelse.[255]

Ud over legalitetskravet, kræves efter artikel 8, stk. 2, at indgrebet er nødvendigt i et demokratisk samfund af hensyn til bl.a. at forebygge uro eller forbrydelser. Uagtet

---

[251] Kjølbro: *"Den Europæiske Menneskerettighedskonvention for praktikere"*, 2017, s. 762, med henvisning til bl.a. *Valenzuela Contreras mod Spanien*, dom af 30. juli 1998, pkt. 46, og *Kennedy mod Storbritannien*, dom af 18. maj 2010, pkt. 155-170, samt Artikel 5: "*Politiets infiltration på digitale platforme – set i et menneskeretligt perspektiv"*, pkt. 4.2.4. og 4.3.

[252] *Petri Sallinen m.fl. mod Finland*, dom af 27. september 2005, pkt. 90.

[253] Se hertil bl.a. dommene *Malone mod Storbritannien*, dom af 2 august 1984, pkt. 67-68, *Amann mod Schweiz*, dom af 16. februar 2000, pkt. 56, samt *Roman Zakharov mod Rusland*, dom af 4. december 2015, pkt. 229-231. Se endvidere Kjølbro: *"Den Europæiske Menneskerettighedskonvention for praktikere"*, 2017, s. 763, og Rainey, B., E. Wicks and C. Ovey: "*The European Convention on Human Rights*", 7th edition, 2017, s. 410 ff., samt Artikel 4: "*Politiets hjemmel til 'hacking' som led i en efterforskning.*"

[254] *Kennedy mod Storbritannien*, dom af 18. maj 2010, pkt. 151-152, med henvisning til *Weber og Saravia mod Tyskland,* afgørelse om realitetsbehandling af 29. juni 2006, pkt. 93-95.

[255] Kjølbro: *"Den Europæiske Menneskerettighedskonvention for praktikere"*, 2017, s. 764, med henvisning til *P.G. og J.H. mod Storbritannien*, dom af 25. september 2001, pkt. 62.

formuleringen angår at 'forebygge', må det lægges til grund, at der heri også er indeholdt, at politiet efterforsker forbrydelser, der *er* sket.[256] I forhold til de hensyn, nævnt i artikel 8, stk. 2, er der tale om en udtømmende opregning af legitime hensyn, der skal fortolkes indskrænkende, hvilket allerede følger af, at der er tale om undtagelser til hovedreglen i stk. 1, men også er udtrykkeligt fastslået i EMD-praksis.[257]

I vurderingen af nødvendighed ligger et proportionalitetsprincip, hvori indgår, om indgrebet sker af hensyn til at forfølge et presserende socialt behov ("a pressing social need"), og om indgrebet er proportionalt i forhold til det konkrete formål.[258] Ved denne afvejning mellem forskellige hensyn, er medlemsstaterne overladt en vis skønsmargin "*margin of appreciation*", hvor EMD viser en vis tilbageholdenhed i prøvelsen, hvilket dog varierer alt efter hvilke rettigheder, der er tale om, karakteren og intensiteten af indgrebet mv.[259]

2.1. Den tekniske adgang i forhold til EMRK artikel 8, stk. 2

Den danske regulering i retsplejeloven af indgrebene, hemmelig ransagning, dataaflæsning og indgreb i meddelelseshemmeligheden, må siges at opfylde legalitetskravet i artikel 8, stk. 2, om lovhjemmel, der er tilgængelig og forudsigelig. Eneste punkt, som ikke er fuldstændig reguleret i retsplejeloven, er samspillet mellem hemmelig

---

[256] *Camenzind mod Schweiz*, dom af 16. december 1997, pkt. 40, og *Van Der Heijden mod Holland*, dom af 3. april 2012, pkt. 54, se hertil Kjølbro: *"Den Europæiske Menneskerettighedskonvention for praktikere"*, 2017, s. 766, og Rainey, B., E. Wicks and C. Ovey: "*The European Convention on Human Rights*", 7th edition, 2017, s. 352 f., jf. Artikel 5: *"Politiets infiltration på digitale platforme – set i et menneskeretligt perspektiv"*, pkt. 4.3.

[257] Se hertil bl.a. *Perinçek mod Schweiz*, dom af 15. oktober 2015, pkt. 151, samt Kjølbro: *"Den Europæiske Menneskerettighedskonvention for praktikere"*, 2017, s. 765, og Rainey, B., E. Wicks and C. Ovey: "*The European Convention on Human Rights*", 7th edition, 2017, s. 341 f.

[258] *Handyside mod Storbritannien,* dom af 7. december 1976, pkt. 48 og 49, *Silver og andre mod Storbritannien*, dom af 25. marts 1983, pkt. 97, samt Rytter: *"Individets grundlæggende rettigheder"*, 2019, s. 105 ff., Kjølbro: *"Den Europæiske Menneskerettighedskonvention for praktikere"*, 2017, s. 767, samt Rainey, B., E. Wicks and C. Ovey: "*The European Convention on Human Rights*", 7th edition, 2017, s. 359.

[259] Se bl.a. *Handyside v. The United Kingdom,* dom af 7. december 1976, pkt. 48 og 49, *Piechowicz mod Polen*, dom af 17. april 2012, pkt. 212, og *Paradiso og Campanelli mod Italien*, dom af 24. januar 2017, pkt. 179-184, samt Rainey, B., E. Wicks and C. Ovey: "*The European Convention on Human Rights*", 7th edition, 2017, s. 360 ff. Begrebet "*margin of appreciation*" indgår tillige i Artikel 2: "*Logning af teledata i lyset af Tele2-dommen*", pkt. 3.2.

ransagning og dataaflæsning, men disse to bestemmelsers anvendelsesområde i relation til politiets 'hacking' kan udledes af Højesterets kendelse i U 2012.2614 H, som der er redegjort for i Artikel 4: "*Politiets hjemmel til 'hacking' som led i en efterforskning*". Det uheldige samspil til trods, må det lægges til grund, at retstilstanden på dette punkt opfylder legalitetskravet i artikel 8, stk. 2. Dette skyldes, at det, der følger af retspraksis blot er den præcise sondring mellem de to indgreb, hemmelig ransagning og dataaflæsning i relation til politiets 'hacking', og at der ikke er tale om, at selve hjemlen og betingelserne for et indgreb skal udledes af retspraksis. Der er i bestemmelserne om hemmelig ransagning, jf. § 799, og om dataaflæsning, jf. § 791 b, og i tilknytning hertil fastsat en række materielle og processuelle betingelser for at begrænse indgrebene til det nødvendige.

Ligeledes for disse tre hemmelige indgreb er der i reguleringen fastsat, at indgrebene kan ske af hensyn til politiets efterforskning af grov kriminalitet, hvorfor også de særlige formål og proportionalitetskravet i artikel 8, stk. 2 er opfyldt.

De detaljerede forskrifter for de tre hemmelige indgrebs varighed og udstrækning synes ligeledes at harmonere med EMRK artikel 8, stk. 2, hvor disse krav som nævnt ovenfor navnlig er udledt i forhold til indgreb i meddelelseshemmeligheden, se eksempelvis *Roman Zakharov mod Rusland*.[260] Ligeledes medvirker de processuelle krav om indgrebsadvokat og underretning til at begrænse indgrebets udstrækning.

3. Er der noget teknisk indgreb, der ikke dækkes af retsplejelovens regulering?

På baggrund af analysen af reguleringen af politiets tekniske indgreb er spørgsmålet, om der er nogen former for tekniske indgreb, der ikke er dækket af retsplejelovens regulering. Her kan indledningsvist peges på det tekniske indgreb, der ligger i, at politiet fra beslaglagte computere og mobiltelefoner kan etablere en fremadrettet, onlineovervågning af bl.a. digitale platforme. Metoden, der enten kan anses som en del af beslaglæggelsen eller som en ny fremadrettet, ransagning, er ikke klart reguleret i retsplejeloven, og der argumenteres derfor for at etablere en klar regulering af metoden i retsplejeloven, jf. Artikel 4: *"Politiets hjemmel til 'hacking' som led i en efterforskning"*, pkt. 5.5.

I det følgende peges på yderligere to områder, hvor det kan diskuteres, om der er tale om et teknisk indgreb, der ikke er dækket af retsplejelovens regulering: Først digital observation og dernæst brud på kryptering. Derefter følger afsnit 4 med retspolitiske overvejelser om nytten af en egentlig hjemmel til politiets 'hacking'.

De tre regelsæt, hemmelig ransagning, dataaflæsning og indgreb i meddelelseshemmeligheden, regulerer som nævnt politiets tekniske *adgang* til private/beskyttede

[260] *Roman Zakharov mod Rusland*, dom af 4. december 2015, pkt. 229-231.

datasystemer, og uanset om dette sker med politiets egne metoder eller med bistand fra en udbyder til et datasystem, vil implicit i rettens kendelse også ligge en tilladelse til, at politiet kan gøre sig bekendt med *indholdet*, hvilket vil sige de oplysninger, der er lagret i datasystemet, eller den aktivitet eller kommunikation, der foregår i systemet. For så vidt angår hvilke tekniske metoder, der konkret skal bruges til at sikre indholdet, er der ikke så meget tvivl ved indgreb i meddelelseshemmeligheden, hvor udbyderen teknisk iværksætter en aflytning eller overvågning af kommunikationen, ligesom en kendelse til dataaflæsning vil indeholde en henvisning til det datasystem og den metode, indgrebet angår.

Bortset herfra, og navnlig relevant ved hemmelig ransagning, er spørgsmålet, om politiet er frit stillet i forhold til inde i det private datasystem at anvende nye tekniske metoder til at optimere indsamlingen af data i et sådant omfang, at der kan blive tale om at 'udvinde' data eller med tekniske værktøjer at etablere en form for overvågning.

I det følgende redegøres for retsplejelovens regler om observation, jf. § 791 a, stk. 1-3, for at undersøge om disse regler også har – eller kan tænkes at få – et digitalt anvendelsesområde, der kunne supplere de tre indgrebshjemler, hemmelig ransagning, dataaflæsning og indgreb i meddelelseshemmeligheden.

3.1. Digital observation

Retsplejelovens § 791 a, stk. 1-3 indeholder en regulering af tre former for observation.[261] Den mildeste form i stk. 1 angår politiets "*fotografering eller iagttagelse ved hjælp af kikkert eller andet apparat af personer, der befinder sig på et ikke frit tilgængeligt sted*", hvilket kan ske, hvis indgrebet må antages at være af væsentlig betydning for efterforskningen, og efterforskningen vedrører en lovovertrædelse, der efter loven kan medføre fængselsstraf.

Bestemmelsens stk. 2 regulerer observation, der sker med mere sofistikerede metoder, således ved hjælp af "*fjernbetjent eller automatisk virkende tv-kamera, fotografiapparat eller lignende apparat*", som kun må foretages, hvis efterforskningen vedrører en lovovertrædelse, der efter loven kan medføre fængsel i 1 år og 6 måneder eller derover.

[261] Reglerne blev indført ved lov nr. 229 af 21. april 1999 på baggrund af Strafferetsplejeudvalgets Bet. 1298/1995 om fotoforevisning, konfrontation, efterlysning og observation (se hertil lovforslag nr. 41 af 8. oktober 1998, pkt. 6.) Senere ændringer i § 791 a, stk. 1-3 angår (bortset fra en enkelt sproglig modernisering) alene konsekvensrettelser som følge af ændringer i straffelovens bestemmelser og strafferammer, samt ændringer i udlændingeloven.

Den mest indgribende form for observation er reguleret i bestemmelsens stk. 3, som angår observation af personer, der befinder sig i en bolig eller andre husrum, "*ved hjælp af fjernbetjent eller automatisk virkende tv-kamera, fotografiapparat eller lignende apparat eller ved hjælp af apparat, der anvendes i boligen eller husrummet*". En sådan observation må kun foretages, såfremt der er bestemte grunde til at antage, at bevis i sagen kan opnås ved indgrebet, og indgrebet må antages at være af afgørende betydning for efterforskningen, og her skal et restriktivt kriminalitetskrav være opfyldt: Efterforskningen skal angå en forbrydelse, der kan straffes med fængsel i 6 år eller derover, eller angå en af de i bestemmelsen særligt nævnte forbrydelser, ligesom det kræves, at efterforskningen vedrører en lovovertrædelse, som har medført eller som kan medføre fare for menneskers liv eller velfærd eller for betydelige samfundsværdier.[262]

Gradueringen i betingelserne angår således dels *lokaliteten*, når politiet observerer "ikke frit tilgængeligt sted" til det mere indgribende observation af "boligen eller husrummet", dels de *metoder*, der bruges til observationen, fra de håndholdte "fotografiapparater" til de "fjernbetjente eller automatisk virkende tv-kameraer" mv. Det mest indgribende angår observation hvor fjernbetjent kamera mv. anvendes til observation af "boligen eller husrummet" eller et "apparat" der anvendes "i boligen eller husrummet", jf. § 791 a, stk. 3. Konteksten for observationsreguleringen har således været fysiske lokaliteter.

Værd at bemærke er imidlertid, at observationen, som er beskrevet i stk. 1, angår den lidt mere diffuse betegnelse "iagttagelse af personer, der befinder sig på et ikke frit tilgængeligt sted." Strafferetsplejeudvalget var opmærksom på, at begrebet kunne volde tvivl, men henviste i den forbindelse til den strafferetlige terminologi og praksis i relation til straffelovens § 264 a, der handler om uberettiget at fotografere personer på ikke frit tilgængeligt sted.[263]

Ved fastlæggelse af rammerne for efterforskningsmetoden observation, anførte Strafferetsplejeudvalget, at der måtte ske en afvejning af på den ene side hensynet til at muliggøre en effektiv efterforskning, og på den anden side hensynet til, at politiets anvendelse af observation ikke får karakter af en systematisk eller utilladeligt indgribende overvågning af borgerne.[264] Udvalget, som sammenlignede observation med indgreb i meddelelseshemmeligheden, fandt, at når også observation foregår

---

[262] Strafferetsplejeudvalget ønskede med fastsættelsen af kriminalitetskravet for den mest indgribende form for observation at følge samme niveau som ved indgreb i meddelelseshemmeligheden, jf. Bet. 1298/1995, pkt. 5.2.5.2.

[263] Bet. 1298/1995, pkt. 5.1., med henvisning til Knud Waaben: *"Strafferettens specielle del"*, 1989, s. 196-197, og Vagn Greve m.fl.: *"Kommenteret Straffelov, Speciel del"*, 1994, s 309.

[264] Bet. 1298/1995, pkt. 5.2.4.

skjult for den, der rammes, øges behovet for at sætte snævre grænser for indgrebets anvendelse.[265]

Processuelt gælder, at politiet er tillagt kompetence til at træffe afgørelse om den milde form for observation, jf. § 791 a, stk. 1. Strafferetsplejeudvalgets inspiration fra indgreb i meddelelseshemmeligheden træder tydeligt frem ved den processuelle ramme for observation efter stk. 2 og 3, da disse indgreb kræver rettens kendelse, ligesom der skal beskikkes en indgrebsadvokat, fastsættes en varighed for indgrebet på maksimalt 4 uger mv., alt jf. § 791 a, stk. 8, der henviser til reglerne for indgreb i meddelelseshemmeligheden.

Til besvarelsen af spørgsmålet om observationsreglerne har et digitalt anvendelsesområde, forstået som en ren anvendelse på internettet, hvor software udgør det "automatisk virkende apparat", der bruges til at iagttage personer på et "ikke frit tilgængeligt område", jf. § 791 a, stk. 2, er svaret på nuværende tidspunkt nej. Der ses ikke at være trykt retspraksis om observation anvendt på digitale platforme. Ved Højesterets kendelse, U 2012.2614 H, er hemmelig ransagning fastslået som den almindelige hjemmel til, når politiet vil gøre sig bekendt med oplysninger i et privat datasystem.[266] I samme retning taler den tidligere "snifferdom", U 2001.1276 H, hvor Højesteret afviste analog anvendelse af observationsreglerne i § 791 a, stk. 3 som hjemmel til, at politiet i mistænktes lejlighed kunne installere et snifferprogram i hans computer, der fortløbende rapporterede om hans aktiviteter. Dette indgreb fandt Højesteret i stedet skulle kvalificeres som gentagen hemmelig ransagning, som der ikke var hjemmel til i retsplejeloven på daværende tidspunkt.[267]

Spørgsmålet er herefter, om der kan tænkes digitale scenarier, hvor en form for digital observation kunne være relevant. Som tidligere nævnt, må de retskendelser, hvor politi og anklagemyndighed tillades at anvende et af de tre tekniske indgreb, hemmelig ransagning, dataaflæsning eller indgreb i meddelelseshemmeligheden, indeholde en teknisk beskrivelse af metoden, hvorved kendelsen kommer til at stå som rammen for det tilladte. Når politiet i Facebook- og Messenger-sagen, U 2012.2614 H, fik rettens tilladelse til hemmeligt at ransage disse brugerprofiler med rette kode, indebar dette en aflæsning og bevissikring af de oplysninger, der var tilgængelige på de to profiler. Uden stillingtagen i retskendelsen ville det have formodningen imod sig, at politiet kunne tage teknologi i brug til at tilgå andre oplysninger, end hvad der var tilgængeligt på de to profiler, f.eks. en form for 'dataudvinding',

[265] Bet. 1298/1995, pkt. 5.2.4.
[266] Jf. Artikel 4: *"Politiets hjemmel til 'hacking' som led i en efterforskning"*, pkt. 4.
[267] Jf. ovenfor om dataaflæsning, Kapitel 1, pkt. 2.3.3., samt Artikel 4: *"Politiets hjemmel til 'hacking' som led i en efterforskning"*, pkt. 3.2., og Lene Wacher Lentz: "Hemmelig ransagning og brevstandsning i den digitale virkelighed", Juristen nr. 1/2016, pkt. 4.4.2.

der også omfattede venner og venners venner, og i så fald måtte sagen skulle forelægges retten på ny. Grænserne for, hvad der konkret, metodisk, teknologisk er tilladt, kan dog være ganske flydende, idet teknologien i mange tilfælde blot kan siges at effektivisere, hvad mennesker skal bruge meget længere tid på selv at klikke sig frem til. Afgørende må formentlig være, om indgrebet ved anvendelse af det teknologiske værktøj ændrer karakter, således at det i omfang bliver mere vidtgående eller for de berørte borgere mere indgribende end forudsat i retskendelsen.

Et muligt anvendelsesområde for digital observation skal snarere findes i de situationer, hvor politiets adgang ikke er sket ved en teknisk adgang efter et af de tre regelsæt, men i stedet ved infiltration, hvor administrator af datasystemet eller den digitale platform har tilladt adgang på baggrund af urigtige oplysninger fra en polititjenestemand under dække. Som det fremgår af Artikel 5: "*Politiets infiltration på digitale platforme – set i et menneskeretligt perspektiv*" og neden for i Kapitel 4, er infiltration pt. ikke reguleret i retsplejeloven, og der gælder således ikke noget kriminalitetskrav, ej heller krav om retskendelse eller varighed for indgrebet mv. Set i det lys vil adgang til et privat, beskyttet datasystem eller en digital platform som følge af infiltration, der efterfølges af indsamling og 'udvinding' af oplysninger ved teknologiske værktøjer, forekomme anderledes problematisk. Som det argumenteres for neden for i Kapitel 4, bør det overvejes at regulere infiltrationen, som i visse tilfælde kan anskues som et sofistikeret 'hacking'-værktøj, men allerede på dette sted må påpeges, at der måske her ved en form for digital observation, eller 'data-udvinding', er et område, som ikke er dækket af den eksisterende regulering af de tekniske indgreb i retsplejeloven.

3.2. Politiets brud på kryptering mv.

Kryptering dækker over forskellige former for sikkerhedsforanstaltninger, man kan lave på sin kommunikation og sine systemer. Mest almindeligt er en vpn-kommunikationsforbindelse, men derudover findes en række andre forskellige krypteringsværktøjer. Sikkerhed er som udgangspunkt godt og gavnligt, når det besværliggør kriminelles 'hacking' og uberettigede adgang, men bagsiden er, at myndigheders adgang i forbindelse med kriminalitetsbekæmpelse tilsvarende besværliggøres. Kryptering i forbindelse med politiets efterforskning udgør derfor grundlæggende et dilemma.

Brud på kryptering har fyldt ganske lidt i den straffeprocessuelle retsudvikling, dog ses i Brydensholt-udvalgets Betænkning 1377/1999 at være gjort nogle overvejelser om kryptering.[268] Således refereres i Betænkningens pkt. 2.2. fra OECD's anbefalinger fra 1997, der fremhævede på den ene side betydningen af kryptering i relation til datasikkerhed og beskyttelse af privatlivet og på den anden side betydningen af, at kryptering ikke udgør en risiko for den offentlige sikkerhed og retsforfølgning,

[268] Betænkningens pkt. 5.2.

uden dog at indeholde mere præcise anvisninger til, hvordan disse modstridende interesser samtidig tilgodeses.[269]

Ved indførelse af bestemmelsen om dataaflæsning i 2002, henviste Justitsministeriet til, at en hjemmel til dataaflæsning *"i nogle tilfælde også ville give politiet mulighed for at læse elektroniske meddelelser, der sendes til eller fra en mistænkt via en computer mv., i tilfælde, hvor dette ellers ikke er muligt, fordi der benyttes kryptering, der medfører at meddelelsen ikke kan "aflyttes" under forsendelsen."*[270] Bortset herfra indeholdt lovforslaget ingen overvejelser om kryptering.

Mens politiets tekniske adgang til et datasystem reguleres af de tre regelsæt, hemmelig ransagning, dataaflæsning og indgreb i meddelelseshemmeligheden, er der ikke særskilt i straffeprocessuelle forarbejder eller litteratur taget stilling til den omstændighed, at politiet for at få adgang kan være nødsaget til at bryde en kryptering.

Der kan argumenteres for, at brud på en kryptering kan siges at ligge implicit i politiets tekniske adgang, med en pendant til den fysiske verden vil det være sammenligneligt med låsesmeden, der kommer med sit værktøj, når en bolig skal ransages, eller at politiet sparker døren til lejligheden ind, eller som i Højesterets nye sager, nævnt oven for i Kapitel 1, afsnit 2.3.4., at politiet bruger ejerens fingeraftryk til at åbne en mobiltelefon. Som Højesteret formulerede det i fingeraftrykskendelserne, skal sådanne adgangsveje ses som et *accessorium*, dvs. som en nødvendig magt for at gennemføre det indgreb, der i øvrigt er hjemmel til og er tilladt i den konkrete situation.

Dog kan der konstateres en forskel fra i hvert fald en del af disse accessorium-situationer, hvor adgangsvejen sker i overværelse af den mistænkte/ejeren eller med dennes vidende, til de situationer, hvor politiet bryder krypteringen for at skaffe sig hemmelig adgang til et datasystem. Sådanne situationer er selvsagt skjult for de berørte. Den efterfølgende underretning, der skal gives om indgrebet til den person, der har rådigheden over datasystemet, jf. retsplejelovens § 791 b, stk. 4, jf. § 788, stk. 1, 3 og 4, vil formentlig ikke altid give hele den tekniske specifikation på, hvordan dataaflæsningen er foregået, herunder om kryptering er brudt og hvordan, ligesom det også må holdes for øje, at stk. 4 giver mulighed for i særlige tilfælde at undlade at foretage underretning.

---

[269] Se endvidere om kryptering, Mads Bryde Andersen og Peter Landrock: "Kryptering og efterforskning", Juristen 1995, s. 306 ff., Mads Bryde Andersen: "*IT-retten*", 2005, s. 186 ff. For en nyere behandling af kryptering i en straffeprocessuel kontekst, se 'LIBE'-rapporten nedenfor.

[270] Lovforslag nr. 35 fremsat den 13. december 2001, pkt. 3.4.2.

Dilemmaet om 'kryptering' har tidligere forekommet i en anden teknologisk kontekst, nemlig i forhold til telekommunikation, hvor også teleselskaberne med tekniske sikkerhedsforanstaltninger ville kunne besværliggøre politiets indgreb i meddelelseshemmeligheden ved telefonaflytning mv. I 1985 blev indført i retsplejelovens § 786, stk. 1 en pligt for postvirksomheder og udbydere af telenet eller teletjenester til at bistå politiet ved gennemførelsen af indgreb i meddelelseshemmeligheden, herunder ved at etablere aflytning af telefonsamtaler m.v.[271] Denne forpligtelse understøttes af telelovens § 10, hvor udbydere af elektroniske kommunikationsnet eller -tjenester til slutbrugere, har pligt til uden udgift for staten at sikre, *"at det tekniske udstyr og de tekniske systemer, som udbyderen anvender, er indrettet således, at politiet kan få adgang til oplysninger om teletrafik og til at foretage indgreb i meddelelseshemmeligheden i form af historisk teleoplysning og historisk udvidet teleoplysning, fremadrettet teleoplysning og fremadrettet udvidet teleoplysning, aflytning og teleobservation, jf. retsplejelovens kapitel 71 og 74, herunder, for så vidt angår fremadrettet teleoplysning og udvidet teleoplysning, at politiet kan få adgang, umiddelbart efter at disse oplysninger registreres."*[272] Det fremgår af logningsbekendtgørelsen, hvilke teledata selskaberne er forpligtede til at opbevare, jf. Artikel 2: *"Logning af teledata i lyset af Tele2-dommen."* Således ses altså i retsplejelovens § 786, stk. 1 en autoritativ regulering af det teknologiske dilemma, hvor teleselskaberne forpligtes til at bistå og facilitere politiets indgreb. Af forarbejderne til bestemmelsen fremgår ikke de store principielle privatlivs- og sikkerhedsovervejelser, hvilket må ses i datidens kontekst, og dette står i klar kontrast til de nutidige, aktuelle, internationale diskussioner om kryptering og sikkerhed.[273]

I internationale fora er kryptering også behandlet som et grundlæggende dilemma, og for at sætte den danske retstilstand i et bredere perspektiv, påpeges i det følgende nogle nylige overvejelser og anbefalinger fra EU-regi, idet det samtidig understreges, at der ikke her på nogen måde er tale om en egentlig analyse af de samlede, internationale eller EU-retlige behandlinger af dette spørgsmål.

I regi af Europaparlamentet er udarbejdet en undersøgelse af udvalgte landes regulering for så vidt angår politiets 'hacking' som led i en efterforskning: *"Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Compa-*

[271] Jf. lov nr. 227 af 6. juni 1985, jf. lovforslag nr. 164 A af 1. februar 1985, jf. Bet. 1023/1984, s. 124 og 217.

[272] Lovbekendtgørelse nr. 128 af 7. februar 2014 om elektroniske kommunikationsnet- og tjenester.

[273] Se om denne forpligtelse for teleselskaberne til indretning af udstyr mv., Søren Sandfeld Jakobsen (red.), Søren Johansen og Christian Bergqvist: "*Teleretten*", 2014, s. 181 ff. Forpligtelsen fremgår tillige af Artikel 3: *"Retsplejelovens regulering af politiets adgang til teledata"*, pkt. 3.1.2.

rison of practices", 2017, Study for the LIBE Committee (European Parliament's Committee on Civil, Liberties, Justice and Home Affairs. Undersøgelsen, der i det følgende omtales som 'LIBE-rapporten', vil også indgå i en perspektivering nedenfor i afsnit 4, hvor det diskuteres, om der kunne være nytte af en egentlig hjemmel til 'hacking'.

Rapporten gennemgår indledningsvist krypteringens dilemma med referencer til debatter og synspunkter fra internationale sammenhænge.[274] Fra rapportens gennemgang skal her kort sammenfattes, at der på den ene side står fortalere for retshåndhævelsen, der bl.a. argumenterer for, at systemudbyderne skal levere krypteringsnøgler, så myndighederne altid har adgang til systemerne via denne form for nøglerække, "key escrow", ligesom det argumenteres for, at systemudbyderne er forpligtet til at lave bagdøre i alle systemer, så myndighederne kan få adgang, og at systemudbyderne til enhver tid skal kunne pålægges at facilitere myndighedernes adgang. Som det anføres i LIBE-rapporten, fik disse synspunkter medvind i årene efter sagen, hvor Apple nægtede at bistå FBI med at få adgang til en iPhone.[275]

På den anden side står fortalere for privacy og sikkerhed, der argumenter for, at disse hensyn vejer tungere, ligesom det anføres, at for hver af disse tekniske muligheder, der står åbne for politiet, bliver der tilsvarende svagere sikkerhed, fordi samme muligheder, bagdøre og svagheder kan udnyttes af kriminelle.[276] I LIBE-rapporten omtales, at sårbarheder i Adobe Flash og Windows i 2015 blev udnyttet til et ondsindet 'hacking'-angreb på en statslig institution i USA.[277] Sårbarheder i datasystemer, navnlig i sådanne almindeligt udbredte programmer, kan være oplagte for ondsindede 'hackere' at udnytte. Digter man videre på det scenarie, kunne man forestille sig, at politiet i samme periode havde udnyttet de samme sårbarheder til 'hacking' i forbindelse med efterforskning af anden kriminalitet, og her ville det etiske spørgsmål selvsagt rejses, om politiet skulle have gjort Adobe og Windows opmærksom på disse sårbarheder og dermed forhindret ondsindede 'hacking'-angreb. Her ligger et nærmest uløseligt dilemma: Hvad er vigtigst, politiets mulighed for

[274] LIBE-rapporten, s. 18 ff.

[275] LIBE-rapporten, s. 19, hvor der henvises til Apple's redegørelse til sine kunder, https://www.apple.com/customer-letter/answers/ og en gennemgang af sagens forløb https://www.digitaltrends.com/mobile/apple-encryption-court-order-news/

[276] Se hertil navnlig Harold Abelson et al.: "Keys under doormats: mandating insecurity by requiring government access to all data and communications", Journal of Cybersecurity, 1(1), 2015, 69-79.

[277] LIBE-rapporten, s. 25, med henvisning til rapport fra sikkerhedsvirksomheden, FireEye: *"Zero-Day Danger: A Survey of Zero-Day Attacks and What They Say About the Traditional Security Model. White Paper"*, 2015, tilgængelig efter anmodning på www.FireEye.com. Angrebet, der blev opdaget af FireEye i april 2015, omtales som "Operation Russian Doll".

'hacking' som led i en efterforskning eller politiets medvirken til at forhindre, at andre 'hacking'-angreb sker?

Anbefalingen i LIBE-rapporten er, at førsteprioriteten er et sikkert internet og sikre datasystemer, dvs. at systemudbyderne ikke skal pålægges at lave bagdøre i systemerne.[278] Man går faktisk så langt som til at anbefale, at i det tilfælde, hvor politiet finder en svaghed ved et system (ofte kaldet "zero-day vulnerabilities"), der kan udnyttes til at få adgang, skal politiet efterfølgende gøre systemudbyderen opmærksom på dette, så svagheden kan repareres.[279] På den måde vil den digitale sikkerhed generelt forbedres. Dette vil dog i princippet betyde, at politiet ikke måtte udnytte samme svaghed to gange. Ifølge LIBE-rapporten har hollandsk ret taget stilling til fænomenet "zero-day vulnerabilities", således at det er fastsat ved lov, at det er tilladt for de retshåndhævende myndigheder at udnytte sådanne sårbarheder til at få adgang, dog må man ikke opkøbe information om sårbarheder, ligesom der er krav om underretning om sårbarheden til systemudbyderen.[280]

I tilknytning til LIBE-rapportens overvejelser om 'hacking'-værktøjer, kan man forestille sig en række etiske overvejelser, politiet må gøre sig i forhold til indkøb af 'hacking'-udstyr og programmer af private virksomheder. Først og fremmest må politiet sikre sig, at virksomheden udviser loyalitet, integritet og diskretion, så der ikke er risiko for bagdøre i produkterne, hvorved sælgeren vil kunne monitorere politiets brug af udstyret og måske sælge disse data til kriminelle. Ej heller må virksomheden udtale sig om, hvilke produkter, der er solgt til hvilke landes politimyndigheder.

Man kan også forestille sig, at der ved indkøb af sådanne værktøjer følger en række kontraktretlige forpligtelser, der for eksempel vil bevirke, at politiet ikke efterfølgende må afsløre metoden i forbindelse med en straffesagen, eller underrette systemudbyderen om sårbarheden ved systemet. På den baggrund kan det være relevant at overveje, hvorvidt sådanne nye tekniske, kontroversielle metoder, skal godkendes fra centralt hold inden ibrugtagning.[281] Derudover kunne det overvejes at indføre en særlig uddannelse af de personer i politiet, der skal stå for 'hackingen'.

Sådanne overvejelser om kryptering og udnyttelse af sårbarheder ved systemer, har ikke hidtil været fremme i en dansk straffeprocessuel kontekst, men vil være værd at inddrage, i det tilfælde hvor lovgiver måtte overveje at udarbejde en egentlig

[278] LIBE-rapporten, s. 13 f.
[279] LIBE-rapporten, s. 14.
[280] LIBE-rapporten, s. 26 og 61, se endvidere rapportens s. 31 f. for en gennemgang af EU's regulering mv. i relation til salg og eksport af 'hacking tools' og overvågningsteknologi.
[281] LIBE-rapporten, s. 60, refererer fra en sådan ordning i fransk ret, hvor nye tekniske efterforskningsmetoder skal juridisk godkendes.

hjemmel til politiets 'hacking'. Hvorvidt der er behov for eller nytte ved en sådan udtrykkelig hjemmel behandles i det følgende.

4. Retspolitiske overvejelser om nytten af en egentlig hjemmel til 'hacking'

På baggrund af analysen af retsplejelovens regulering af det tekniske indgreb er der navnlig grund til at gøre op med det uheldige samspil mellem hemmelig ransagning og dataaflæsning, hvor reglernes anvendelsesområde beror på en teknisk redegørelse for, om der er tale om et 'program', jf. dataaflæsning, eller en anden metode, hvor reglerne om hemmelig ransagning gælder, jf. Artikel 4: "*Politiets hjemmel til 'hacking' som led i en efterforskning*." Dette samspil er navnlig uheldigt, når kriminalitetskravet ikke er det samme for de to indgreb, hvor hemmelig ransagning kun tillades i ganske få nævnte former for kriminalitet, mens dataaflæsning som hovedregel kræver 6 års fængsel i strafferammen.[282]

Når lovgiver formodentlig på et tidspunkt vil 'reparere' dette uheldige samspil i reguleringen, kunne der være grund til at etablere dataaflæsning som hjemmel for al den digitale aflæsning, som politiet selv kan foretage uden udbyderens medvirken, og dermed lade sådanne indgreb udgå af anvendelsesområdet for hemmelig ransagning.[283] Om denne nyaffattelse skulle betegnes 'dataaflæsning' eller 'hacking' er af mindre betydning, når blot den digitale kontekst grundigt overvejes, og der etableres en fyldestgørende, detaljeret regulering af dette indgreb.

Ved vurderingen af intensiteten ved politiets 'hacking', kan det først anføres, at borgeren i de fleste tilfælde vil opleve det som mere indgribende at få hemmeligt ransaget sin bolig, end at politiet 'hacker' borgerens digitale system, hvilket taler for at udskille indgrebet fra reglerne om hemmelig ransagning.[284] Navnlig må det være mindre indgribende, når det system, der 'hackes', er brugerprofiler på Facebook og Messenger, jf. U 2012.2614 H, hvor borgeren i forvejen har samtykket til brugervilkår om, at platformene i vidt omfang kan bruge og videregive private oplysninger.[285] Dog må det haves in mente, at vi på vores datasystemer, computere, mobiltelefoner og digitale platforme, samler og lagrer store mængder data, det kan være i form af kommunikation, men også bare browserhistorikken på hjemmesider og søgeord kan være meget følsomme oplysninger for den enkelte.

---

[282] Jf. Artikel 4: *"Politiets hjemmel til 'hacking' som led i en efterforskning"*, pkt. 4.1., og Lene Wacher Lentz: "Hemmelig ransagning og brevstandsning i den digitale virkelighed, Juristen nr. 1/2016, pkt. 4.5.

[283] Artikel 4: "*Politiets hjemmel til 'hacking' som led i en efterforskning*", pkt. 4.2.

[284] Jf. Lene Wacher Lentz: "Hemmelig ransagning og brevstandsning i den digitale virkelighed, Juristen nr. 1/2016, pkt. 4.5.

[285] Artikel 4: "*Politiets hjemmel til 'hacking' som led i en efterforskning*", pkt. 4.2.

Politiets 'hacking', hvor der indsamles oplysninger, kan dog i nogle sammenhænge være et mere intensivt og omfattende indgreb, end de traditionelle indgreb som indgreb i meddelelseshemmeligheden og hemmelig ransagning, idet disse 'hacking'-værktøjer kan 'udvinde' *alle* data i et konkret datasystem, og således i visse tilfælde sikre helt enorme mængder data på meget kort tid. I LIBE-rapporten henvises til et eksempel fra 2017, hvor hollandsk politi skaffede sig adgang til – og dekrypterede – syv terabytes (TB) data lagret på en server, tilhørende det hollandske firma Ennetcom.[286] For at få en idé om omfanget, skønnes éen TB at kunne indeholde omkring 86 millioner sider i Microsoft Word-formatet eller 310.000 billeder.[287]

Ved de retspolitiske overvejelser, som lovgiver må gøre sig, om en mulig særlig regulering af politiets 'hacking', er det relevant både at inddrage politiets og anklagemyndighedens praktiske erfaringer, samt overvejelse af mulige tekniske scenarier, ligesom der må indhentes inspiration fra andre landes lovgivning og internationale fora. I den forbindelse henledes opmærksomheden på LIBE-rapporten fra 2017, som indeholder en analyse af seks udvalgte EU-landes og tre ikke-EU-landes regulering af politi-'hacking', der blev sammenholdt med EMRK artikel 8 og Chartrets artikel 7 krav til indgreb i privatlivets fred, og på den baggrund opstilles i rapporten en række anbefalinger til 'best practice' for reguleringen af dette område. For at illustrere de mange overvejelser i tilknytning til en regulering af politiets 'hacking', man endnu har til gode at gøre sig i en dansk kontekst, kan det påpeges, at det i LIBE-rapporten anbefales, at staterne i deres retsgrundlag for 'hacking' bevæger sig væk fra "grey area"-reguleringer, hvorved forstås traditionelle, brede indgrebshjemler, f.eks. til ransagning, da disse ikke tager højde for det meget indgribende ved politiets 'hacking' og ikke giver den fornødne klarhed og præcision for sådanne indgreb.[288] Desuden anbefales det, at det i national ret sikres, at 'hacking' målrettes mest muligt mod det nødvendige for efterforskningen, og at 'hacking' i form af masseindsamling af data ("bulk or untargeted use of hacking") forbydes.[289]

4.1. Tekniske aspekter ved politiets 'hacking'

Allerede under den nugældende danske retstilstand, hvor domstolene tager stilling til anklagemyndighedens begæringer om tilladelse til 'hacking', hvad enten det er i form af hemmelig ransagning eller dataaflæsning, er der et teknisk element, som retten må forholde sig til. Ved beskrivelsen af de tekniske metoder, hvor der kan

[286] LIBE-rapporten, s. 22, med henvisning til Pierluigi Paganini: "*Ennetcom – Dutch Police confirmed to have decrypted BlackBerry PGP messages in a criminal case*", Article on Security Affairs, 10 March 2017.
[287] LIBE-rapporten, s. 22, med henvisning til Kelly Brown: *"A Terabyte of Storage Space: How Much is Too Much?"*, University of Oregon blog: The Information Umbrella: Musings on Applied Information Management, 2014.
[288] LIBE-rapporten, s. 69.
[289] LIBE-rapporten, s. 69.

være tale om at anvende rette adgangskode, bryde kryptering, installere eller fremsende malware programmer (trojanere mv.) til computere og datasystemer eller udnytte sårbarheder ved systemet mv., må retten kvalificere det konkrete indgreb. I den forbindelse må vurderes den efterforskningsmæssige nytte og nødvendighed ved 'hackingen', men også indgrebets intensitet, navnlig i forhold til hvor mange udenforstående det kan berøre, foruden de sikkerhedsmæssige overvejelser om, hvordan 'hackingen' stoppes, udstyret fjernes mv.

Jo mere retten går i dybden med de tekniske aspekter ved indgrebet og beskriver den tekniske metode og rammerne for indgrebet i kendelsen, jo klarere et grundlag har politiet at arbejde efter. Når 'hackingen' derefter iværksættes, må politiet så detaljeret som muligt beskrive denne tekniske efterforskning i politirapporter, både af hensyn til de personer og systemer, der berøres, og af hensyn til de personer, der måtte blive strafforfulgt på baggrund af beviser, der fremkommer ved indgrebet. Under en straffesag skal det være muligt for retten og den beskikkede forsvarer at vurdere indgrebets omfang og intensitet og de bevismæssige resultater derfra. Dog kan politiet have en interesse i at hemmeligholde den præcise 'hacking'-metode af hensyn til senere brug i andre sager. Det vil her være op til domstolene at foretage en afvejning af hensyn og sikre, at sigtede og dennes forsvarer får den rette mængde information til at kunne varetage forsvaret.

Sådan som politiets 'hacking' nu er reguleret i retsplejelovens bestemmelser om hemmelig ransagning og dataaflæsning, er der ikke nogen detaljerede forskrifter på, hvordan hackingen må foregå. Såfremt det af lovgiver overvejes at etablere en egentlig 'hacking'-hjemmel, må der tillige tages stilling til de typisk forekommende scenarier i tilknytning hertil.

Som tidligere nævnt i relation til observation, er det ikke i de to indgrebshjemler, hemmelig ransagning og dataaflæsning fastsat, hvad politiet, efter at have fået adgang, konkret må foretage sig inde i systemet.[290] Det må implicit i retskendelsen ligge, at politiet må gøre sig bekendt med data, dekryptere data, kopiere og sikre data og følge kommunikation og aktivitet i realtid. Men spørgsmålet er, i hvilket omfang politiet må påvirke dét, de finder, herunder om politiet må forvanske eller slette data, og om de må sende data til udenforstående fra det computersystem, der er skaffet adgang til ("som om ejeren har sendt det"). Af yderligere tekniske overvejelser man må gøre sig, er om politiet må ændre de tekniske indstillinger i systemet, hvor det vil være særlig indgribende, hvis politiet kan aktivere mikrofon og/eller kamera i en computer, der således i realiteten vil realisere både en rumaflytning, jf. § 780, stk. 1, nr. 2, og en observation af bolig, jf. § 791 a, stk. 3. Dette rejser også spørgsmålet, om politiet har pligt til at slå mikrofon og/eller kamera fra, hvis det

[290] Jf. ovenfor afsnit 3.1.

allerede er aktiveret. Endelig er spørgsmålet, om politiet har pligt til at fjerne programmet efterfølgende og hvordan det i øvrigt sikres, at politiets 'hacking' ikke gør skade på systemet, eksempelvis ved at skabe en uberettiget adgang for andre.[291]

5. Sammenfatning vedrørende politiets tekniske indgreb

Til forskningsspørgsmålet om, hvordan reguleringen er af politiets tekniske tvangsindgreb på private områder på internettet, kan det konstateres ud fra det straffeprocessuelle legalitetsprincip – både efter Hans Gammeltoft-Hansens definition og EMRK artikel 8 – at politiets teknisk 'hacking'-indgreb i private datasystemer kræver klar lovhjemmel, jf. Artikel 4: *"Politiets hjemmel til 'hacking' som led i en efterforskning"*, pkt. 2.

Hvorvidt der er tale om offentligt tilgængelige data, som politiet umiddelbart kan gøre sig bekendt med, jf. politilovens § 2 a, eller om der er tale om private data og systemer, kan meget ofte være en ganske vanskelig vurdering. Dette illustreres i Artikel 1: *"'Hacking' og det digitale privatliv*", som ud fra en analyse af straffelovens § 263 om 'hacking' undersøger grænsefladen mellem offentligt og privat område på internettet. Navnlig IT-'hackeren', der undersøger systemer og de sociale medier som ny digital kontekst, indebærer en vanskelig grænsedragning, som også vil være en udfordring for politiet i efterforskningen på internettet.

Selve det tekniske tvangsindgreb reguleres af tre regelsæt i retsplejeloven – hemmelig ransagning, dataaflæsning og indgreb i meddelelseshemmeligheden – hvor der i afhandlingen retspolitisk argumenteres for en ny samlet bestemmelse, der regulerer politiets hjemmel til 'hacking', således at der gøres op med et uheldigt samspil mellem hemmelig ransagning og dataaflæsning, og således at den nye bestemmelse mere præcist kan regulere 'hacking'-indgrebet og den digitale kontekst, og således at typiske 'hacking'-scenarier og aspekter omkring kryptering overvejes. Ved samme lejlighed bør ligeledes reguleres, at politiet har mulighed for via beslaglagte mobiltelefoner og computere at etablere en ganske omfattende, fremadrettet, onlineovervågning, jf. Artikel 4: *"Politiets hjemmel til 'hacking' som led i en efterforskning"*, pkt. 5.

Derudover er påpeget et område om digital observation, hvorved i denne kontekst forstås en teknologisk 'udvinding' af data på private, digitale platforme, hvilket som tidligere nævnt, navnlig vil være relevant i de tilfælde, hvor politiet har skaffet sig

[291] Som inspiration til nogle af disse overvejelser kan inddrages de norske bestemmelser om dataaflæsning i straffeprosesslovens § 216 o og § 216 p, se hertil om de tekniske aspekter, Prop 68 L, (2015-2016) om Endringer i straffeprosessloven mv. (skjulte tvangsmidler), pkt. 14.8. Departementets vurderinger, navnlig s. 264 ff. Se endvidere Ingvild Bruce og Geir Sunde Haugland: *"Skjulte tvangsmidler"*, 2. utgave, 2018, s. 251 ff.

adgang til en digital platform ved infiltration, hvorefter politiet ønsker at anvende sofistikeret software til at 'udvinde' data. Om infiltration og de øvrige 'menneskelige indgreb', følger nærmere i næste kapitel.

Kapitel 4 Reguleringen af politiets 'menneskelige indgreb' på internettet

1. Sammenfattende om politiets 'menneskelige indgreb'

Når en polititjenestemand med et efterforskningsmæssigt formål har kontakt til borgeren uden at give sig til kende som politi, vil dette være omfattet af efterforskningsmetoden 'infiltration'. Derudover kan yderligere to metoder realiseres afhængig af, om politiet opstiller en fristelse for borgeren, hvilket er omfattet af lokkedue-situationen, eller politiet bistår ved en forbrydelse, hvilket er omfattet af agentvirksomhed. I denne afhandling betegnes disse tre metoder som politiets 'menneskelige indgreb', jf. om dette begreb neden for i afsnit 5.

Infiltration, som blev undersøgt i Artikel 5: *"Politiets infiltration på digitale platforme – set i et menneskeretligt perspektiv*", kan i den digitale variant indeholde flere aspekter, der hver for sig kan udgøre et indgreb i borgerens privatliv, korrespondance mv., jf. EMRK artikel 8, stk. 2, eksempelvis indsamling og registrering af borgerens oplysninger. Derudover kan infiltration, når det bruges til under urigtige foregivender at få adgang til private, digitale platforme, systemer mv., anskues som en form for avanceret 'hacking'-metode, hvor der til sammenligning gælder en ganske restriktiv regulering af den tekniske 'hacking'. I artiklen argumenteres for en regulering af infiltration som efterforskningsmetode.

I Artikel 6: "*Politiagenter i et menneskeretligt perspektiv*" er analyseret den danske regulering af agentvirksomhed i retsplejelovens § 754 a ff., hvor der opfordres til en genovervejelse af den processuelle ramme for at sikre, at agentvirksomhed kun iværksættes og opretholdes til det strengt nødvendige for at sikre bevis for den kriminalitet, der efterforskes. Således anbefales nærmere indførelse af advokatbeskikkelse, en begrænsning på varigheden af agentaktionen, som det kendes fra de hemmelige tvangsindgreb, telefonaflytning mv. Et skærpet fokus på agentaktioner understøttes af praksis fra EMD, som har forholdt sig restriktivt til gentagne eller fortløbende agentaktioner.

Lokkedue-situationen, som har en tæt sammenhæng med både infiltration og agentvirksomhed, er kun ganske kort berørt i Artikel 5 og Artikel 6. I det følgende afsnit uddybes metoden.

2. Lokkedue-situationen

Da metoden blev beskrevet i Betænkning 1023/1984, angik et af eksemplerne en kvindelig polititjenestemand, der går i en park, hvor der tidligere er blevet begået

voldtægtsforbrydelser, og politiet dermed spiller 'offer' for en mulig gerningsmand.[292] Det 'fristelsesmoment', der heri indgår, vil kun formå ganske få personer til at begå en så alvorlig forbrydelse. Det andet eksempel i Betænkningen angår *"henstillen af ting af en art, der tidligere har været genstand for tyveri, på et sted, hvor politiet kan observere dem og iagttage, hvem der stjæler dem."*[293] Dette eksempel, som ikke hidtil er blevet problematiseret, må dog siges at indeholde et fristelsesmoment, der rammer bredere og betydeligt flere borgere. Eksemplet forekommer ikke helt velvalgt.

Når efterladte værdier i gadebilledet indeholder en fristelse for en hel del 'almindelige' mennesker, kan man først spørge, hvorfor politiet dog skulle foretage en sådan handling. Det er ikke politiets opgave at efterlade værdigenstande som fristelser i almindelighed og dermed frembringe flere tyverier, end der i øvrigt forekommer i samfundet. EMD ses ikke på nuværende tidspunkt i sin praksis at have taget stilling til sådanne 'almindeligt' udlagte fristelser, som Lijana Štarienė har eksemplificeret ved, at politiet efterlader en taske i parken eller henstiller en lastbil med cigaretter åbnet og uden opsyn, i begge tilfælde for at kunne anholde en tyv.[294] Der kan dog argumenteres for, at politiet i en situation, hvor der ikke er et forudgående mistankegrundlag eller en efterforskningsmæssig anledning til at udlægge en sådan 'almindelig' fristelse, fremprovokerer en forbrydelse, der ellers ikke ville være blevet begået, jf. EMRK artikel 6, stk. 1.

At politiet skulle henstille en sådan fristelse ville kun give mening, hvis det skete på baggrund af en konkret mistanke, eksempelvis relateret til et bestemt sted eller rettet mod bestemte personer, og aktionen dermed havde et særligt efterforskningsmæssigt formål. Et bedre lokkedue-eksempel ville således være, hvis politiet hensatte en aflåst bil af eksklusivt mærke isat gps-sender på en parkeringsplads, hvor der har været mange biltyverier. En dyr, men aflåst bil, vil kun friste de få, der ved, hvordan man bryder ind i bilen, borttager den uden nøgle, og eventuelt senere afsætter den. Dette er ikke en fristelse, der rammer tilfældige personer, det er en målrettet, iscenesat pågribelse. Aktionen sker på baggrund af en konkret mistanke og med et efterforskningsmæssigt formål. Et sådant tilfælde, hvor det vil være muligt for politiet at anholde en gerningsmand på fersk gerning, og hvor der ikke er nogen

[292] Bet. 1023/1984, s. 160 f.
[293] Bet. 1023/1984, s. 160 f.
[294] Jf. Lijana Štarienė: "The limits of the use of undercover agents and the right to a fair trial under Article 6(1) of the European Convention on Human Rights", University of Wroclaw, Jurisprudence, 2009, 3(117), p. 263-284, pkt. 1.3.

interageren mellem politiet og de mistænkte, frembringer ikke de betænkeligheder, som er baggrunden for agentreguleringen.[295]

Retsplejelovens skelnen mellem lokkedue-situationen og agentvirksomhed kan i visse tilfælde forekomme mindre velbegrundet, hvilket Lasse Lund Madsen på baggrund af U 2012.2225 Ø har illustreret med en politiagent på digitale platforme, der under dække kommunikerer med en person, der ønsker seksuelt samkvem med et barn.[296] I de tilfælde hvor politiagenten indtager rollen som offer (eksempelvis mindreårig) er dette omfattet af lokkedue-situationen og dermed ikke underlagt nogen regulering. Indtager politiagenten i stedet rollen som medgerningsmand, der bistår med at arrangere et møde med et barn, er situationen omfattet af agentreglerne, uagtet 'fælden' der lægges for den mistænkte er fuldstændig den samme.[297] Som Lund Madsen også har påpeget, sondrer EMD ikke mellem, om undercover-agenten udgiver sig for at være offer eller gerningsmand, og dansk ret må bringes i overensstemmelse hermed.[298] Det kan i øvrigt konstateres, at Gammeltoft-Hansen som mindretal i Strafferetsplejeudvalget indtog det synspunkt, at også lokkedue-situationen skulle reguleres, idet situationen ligeledes frembød fristelsesmomenter.[299]

På baggrund af den klassiske lokkedue-situation med kvinden i parken og ovennævnte eksempel om bilen på parkeringspladsen, er det dog vanskeligt at begrunde, at alle situationer, hvor politiet har iscenesat en form for fristelse for borgeren, skulle være omfattet af den restriktive regulering af agentvirksomhed. Det kræver nærmere overvejelser at fastslå, hvilke lokkedue-situationer, der ligner agentvirksomhed så meget, at de tillige skal være omfattet af reguleringen. Umiddelbart synes skillelinjen mellem de mere almindelige iscenesatte pågribelser og de problematiske 'fælder', dels at have at gøre med, hvilken form for fristelsesmoment der iscenesættes og på hvilken konkret mistanke- og efterforskningsmæssig baggrund, dels i hvor høj grad politiet har interageret og kommunikeret med borgeren og påvirket denne i retning af forbrydelsen.

Sammenfattende kan det konstateres, at den danske agentregulering med sin medvirken-formulering er for snæver i forhold til retstilstanden efter EMRK artikel 6, stk. 1, idet flere lokkedue-situationer kan realisere EMD's provokationsforbud om, at politiet ikke må tilskynde borgeren til at begå en forbrydelse, der ellers ikke ville være

[295] Jf. hertil også Lund Madsen i U 2017B.95, s. 99, som anfører, at der i Betænkningens lokkedue-eksempler ikke er en egentlig interaktion mellem lokkeduen og forbryderen.
[296] U 2017B.95, s. 101 f., samt Artikel 6: *"Politiagenter i et menneskeretligt perspektiv"*, pkt. 4.2.
[297] Jf. Artikel 6: *"Politiagenter i et menneskeretligt perspektiv"*, pkt. 4.2.
[298] U 2017B.95, s. 101 f.
[299] Jf. Bet. 1023/1984, s. 161 f. og 223.

blevet begået.[300] Stadig vil en del af lokkedue-situationerne dog være uproblematiske. Retspolitisk set kan det overvejes, om det ikke ville være mest befordrende for den danske strafferetsplejes overensstemmelse med de menneskeretlige standarder, om provokationsforbuddet i retsplejeloven bringes nærmere den definition, som EMD har fastlagt i medfør af EMRK artikel 6, stk. 1.

3. Infiltration i et forvaltningsretligt perspektiv

Som det fremgår af Artikel 5: *"Politiets infiltration på digitale platforme – set i et menneskeretligt perspektiv"*, pkt. 2, beror det retlige grundlag for politiets infiltration på 1984-Betænkningens eksempler og Strafferetsplejeudvalgets samtidige tilkendegivelse af, at sådan infiltration ikke skulle lovreguleres, men måtte betragtes som 'almindelig efterforskning', jf. retsplejelovens § 742, stk. 2, og at lovgiver autoritativt har bekræftet denne opfattelse. Det konkluderes, at der er behov for at fastlægge nogle overordnede rammer for politiets infiltration, der vil opfylde legalitetskravet i EMRK artikel 8, stk. 2.[301]

Som et forvaltningsretligt perspektiv til at illustrere, hvor langt politiets ulovregulerede infiltration på digitale platforme i en straffeprocessuel kontekst befinder sig fra de almindelige principper, der gælder for myndighedsudøvelse i forvaltningen, inddrages i det følgende Ombudsmandens udtalelse i FOB 2011.1501.

3.1. Skattemedarbejder på Facebook, FOB 2011.1501

Som led i SKAT's kontrol af skattepligtsforholdene hos en tredjemand opstod der spørgsmål om personens tilknytning til en kvinde. En medarbejder hos SKAT anvendte herefter sin private Facebook-profil til at indsamle oplysninger om kvinden fra hendes Facebook-profil. Spørgsmålet for ombudsmanden angik, hvorvidt SKAT havde beføjelse til at indsamle oplysninger via Facebook om hende.

Ombudsmanden anførte, at der i almindelighed er et krav om, at offentlige myndigheder legitimerer sig/identificerer sig som offentlige myndigheder, når de henvender sig til borgerne, herunder indsamler oplysninger ved henvendelse til borgerne. Dette altovervejende udgangspunkt var dog ifølge ombudsmanden ikke relevant i de særlige tilfælde, hvor borgeren ikke selv vil kunne konstatere, at en offentlig myndighed har indsamlet oplysninger om ham eller hende. På den baggrund fandt ombudsmanden ikke grundlag for kritik af fremgangsmåden i den konkrete sag, henset til at borgerens profil var åben og oplysningerne dermed offentligt tilgængelige, ligesom ombudsmanden lagde vægt på, at SKAT's medarbejder ikke anvendte en falsk

[300] Jf. Lund Madsen i U 2017B.95, s. 101 f., samt Artikel 6: *"Politiagenter i et menneskeretligt perspektiv"*, pkt. 4.2.
[301] Artikel 5: *"Politiets infiltration på digitale platforme – set i et menneskeretligt perspektiv"*, pkt. 5.

profil og ikke anmodede om borgerens venskab via Facebook. Ombudsmanden anførte herefter, at sagen havde stillet sig anderledes, hvis medarbejderen i SKAT havde anvendt en falsk profil til at indsamle oplysningerne, hvilket begrundes med, at offentligt ansatte ikke *"må, bevidst eller uagtsomt, videregive oplysninger, der er urigtige eller vildledende, eller medvirke til at andre gør det. Denne forpligtelse til sandhed følger af tjenesteforholdet, og pligten gælder derfor i alle forhold, hvor medarbejderen optræder i sin egenskab af offentligt ansat, og det ville være i strid med medarbejderens sandhedsforpligtelse, hvis medarbejderen havde anvendt en falsk profil på Facebook til på SKAT's vegne at indsamle oplysninger om borgeren."*[302]

Ombudsmanden har her anlagt nogle ret restriktive forudsætninger for den forvaltningsretlige adgang til at indsamle oplysninger om borgeren på de digitale platforme. Således forudsættes det, at borgeren har en åben profil, dog kan ifølge Ombudsmanden også oplysninger fra en profil med begrænset tilgængelig profil efter omstændighederne betragtes som offentligt tilgængelige, hvis den pågældende har et meget stort antal 'venner' på Facebook.[303] Desuden forudsættes det, at den offentligt ansatte ikke anvender en falsk profil, men anvender sin egen profil.

Her er det relevant at drage en parallel fra Ombudsmandens vurdering af undersøgelsesmetoden til politiets efterforskningsmetode, infiltration, dog må det haves i erindring, at der udgangspunkt gælder forskellige retlige rammer for metoden, om der er tale om en skattemedarbejder, der ved sin undersøgelse må overholde retssikkerhedsloven,[304] eller en polititjenestemand, der efterforsker forbrydelser efter retsplejeloven. I begge tilfælde er der dog tale om forvaltningspersonel, og de forvaltningsretlige principper gælder som udgangspunkt også for polititjenestemænd. Desuden kan det anføres, at skattemedarbejderens undersøgelse og kontrol af borgerens forhold ret beset kan udgøre de indledende stadier til et forhold, der senere kan overgå til strafforfølgning hos politiet. Begge funktioner er udtryk for myndighedsudøvelse og retshåndhævelse.

---

[302] Ombudsmanden henviste her til "Fagligt etiske principper i offentlig administration", Betænkning afgivet af DJØF's fagligt etiske arbejdsgruppe i september 1993, s. 81, og til "Betænkning nr. 1443/2004 om Embedsmænds rådgivning og bistand", afgivet af Udvalget om embedsmænds rådgivning og bistand til regeringen og dens ministre, s. 142. Endvidere om sandhedspligten i forhold til embedsmænd i centraladministrationen: "Kodex VII – Syv centrale pligter", udgivet af Moderniseringsstyrelsen, samt Sten Bønsing: "Embedsmænds pligter -en kommentar til "Kodex VII – Syv centrale pligter for embedsmænd i centraladministrationen", U 2016.B.33. Se endvidere "God Adfærd i det Offentlige", udgivet af Moderniseringsstyrelsen, KL og Danske Regioner, revideret vejledning 2017.

[303] Se hertil Artikel 1: *"'Hacking' og det digitale privatliv"*, pkt. 5.2.

[304] Lov nr. 442 af 9. juni 2004 om retssikkerhed ved forvaltningens anvendelse af tvangsindgreb og oplysningspligter.

De forudsætninger, Ombudsmanden i FOB 2011.1501 fastlagde for SKAT's medarbejder – og offentligt ansatte i øvrigt – har politiet ikke været omfattet af, som følge af den særlige adgang for politiets infiltration som 'almindelig efterforskning', der blev fastlagt i Bet. 1023/1984. Med støtte heri har politiet udført infiltration ved oprettelse af falske profiler på digitale platforme, og det er i den forbindelse ganske givet også forekommet, at borgere er anmodet om venskab eller lignende uden at kende til den 'politi-identitet', der rettelig kommunikeres med.

I lyset af de restriktive rammer, der ifølge FOB 2011.1501 gælder for SKAT's medarbejdere og offentligt ansatte i det hele taget, om at man som altovervejende hovedregel skal legitimere sig i mødet med borgeren, og at der gælder en sandhedspligt, forekommer politiets ulovregulerede infiltration indgribende og utidsvarende. Det forvaltningsretlige perspektiv fra FOB 2011.1501 synes yderligere at bekræfte det synspunkt, at der må skabes klarere rammer for politiets infiltration, jf. konklusionen i Artikel 5: *"Politiets infiltration på digitale platforme – set i et menneskeretligt perspektiv.*"

3.2. Offentlige myndigheders undersøgelser på kommercielle platforme

Et andet aspekt i FOB 2011.1501 var, at klageren havde henvist til Facebooks standard-vilkår, hvoraf bl.a. fremgår, at man ikke må oprette profiler baseret på urigtige personlige oplysninger, og såfremt der indsamles oplysninger om andre brugere kræves indhentelse af deres samtykke mv. Ombudsmanden udtalte i relation hertil, at SKAT som forvaltningsmyndighed er underlagt en række offentligretlige regler og grundsætninger, som ikke kan fraviges ved aftale, her i form af brugeraftaler med Facebook. Ombudsmanden fremhævede, at SKAT er underlagt officialprincippet samt persondataloven, og i det *"omfang SKAT har offentligretlig hjemmel til at indsamle/behandle oplysninger, viger Facebooks standardvilkår. De vilkår, Facebook har opstillet for brugen af det sociale medie, har således ingen selvstændig betydning i forhold til de offentligretlige regler og grundsætninger, der gælder i Danmark."*

De forudsætninger, Ombudsmanden har indlagt for offentligt ansattes indhentelse af oplysninger fra Facebook, vil Facebook formentlig ikke tage anstød af, ej heller i konkrete situationer gribe ind overfor. Dette beror først og fremmest på, at den offentligt ansatte ikke havde oprettet en profil med urigtige profiloplysninger. Dertil kommer, at Facebook i flere sammenhænge har tilkendegivet at ville samarbejde med myndigheder i relation til retshåndhævelse, hvilket også fremgår af deres brugervilkår, uden at de nærmere omstændigheder herved dog er offentligt kendte. I mangfoldigheden af kommercielle, fortrinsvist udenlandske digitale platforme med forskellig åbne og mere skjulte interesser, er der dog andre platforme med større fokus på privatliv, fortrolighed og anonymitet, herunder platforme på "dark web",

hvor offentligt ansattes undersøgelser eller politiets infiltration, agentvirksomhed mv., ikke ville blive set på med velvilje.

Ombudsmanden ses i FOB 2011.1501 at have anlagt en 'autoritativ', offentligretlig tilgang til Facebook som en af disse platforme. I det praktiske operative arbejde, hvor politiets efterforskning sker på digitale platforme, må man i vidt omfang overholde de vilkår, der opstilles af de kommercielle udbydere. I den forbindelse må politiet fra sag til sag vurdere, om det er nødvendigt og forsvarligt at orientere platformen om infiltrationen og den igangværende efterforskning. I fald politiet ikke overholder platformens vilkår, løber man en risiko for opdagelse, og at udbyderen offentligt eksponerer politiets efterforskning og konkrete metoder, ligesom politiet kan risikere, at udbyderen laver yderligere sikkerhedsforanstaltninger på platformen, hvilket kan vanskeliggøre fremtidigt efterforskningsarbejde.

4. Agentvirksomhed i et digitalt perspektiv

Der er ved agentvirksomhed, både i forhold til den danske regulering og i forhold til EMD's righoldige praksis på området, utallige aspekter, man kan forholde sig til. Ved arbejdet med analysen af agentreguleringen, er udvalgt det mest presserende perspektiv til Artikel 6: *"Politiagenter i et menneskeretligt perspektiv"*, nemlig det processuelle og menneskeretlige perspektiv, og hvordan det i højere grad kan sikres, at agentaktioner begrænses til det strengt nødvendige.

Talrige andre aspekter er her fravalgt, mest iøjnefaldende i forhold til denne afhandlings problemformulering og forskningsspørgsmål er, at de digitale aspekter ved agentvirksomheden er nedtonet i Artikel 6: *"Politiagenter i et menneskeretligt perspektiv"*. Baggrunden herfor er det lovforslag (L 197), der omtales i Artikel 6, og som blev fremsat den 13. marts 2019 om udvidet adgang til agentvirksomhed på internettet, med planlagt tredjebehandling den 16. maj 2019. Lovforslaget gav anledning til adskillige strategiske overvejelser, men da forslaget bortfaldt i forbindelse med folketingsvalget i juni 2019, forekom det mest aktuelt og relevant at holde fokus i artiklen på de processuelle og menneskeretlige aspekter, hvilket også vil have betydning ved en eventuel genfremsættelse af lovforslaget. Det følgende afsnit indeholder en perspektivering af agentvirksomhed i en digital kontekst.

4.1. Digitale udfordringer og retlig regulering

Efterforskningen af strafbare forhold på internettet er vanskelig, når politiet skal afdække, hvem der står bag en annonce eller en profil på de digitale platforme. Politiet vil skulle rekvirere brugeroplysninger fra platformen, men her kan det vise sig, at brugeren har brugt fiktivt navn, telefonnummer fra et registreret taletidskort, ligesom man ved forskellige internettjenester kan sløre sin IP-adresse og dermed fra

hvilket land og hvilken internetudbyder, der kommunikeres fra.[305] Inden politiet får indhentet oplysninger fra platformen, eventuelt efter retskendelse, kan annoncen eller profilen være slettet og 'sporet være koldt'. Tid er således en vigtig faktor. Efterforskningsmæssigt efterspørges en mulighed for, at politiet her og nu kan reagere på annoncer og mistænkelige forhold på digitale platforme, og på denne måde få en kontakt til og et møde i stand med gerningsmanden, der vil kunne anholdes. Dette var baggrunden for den udvidede adgang til agentvirksomhed, som L 197 lagde op til, og som angik fire former for kriminalitet begået ved brug af internettet, jf. Artikel 6: "*Politiagenter i et menneskeretligt perspektiv*", pkt. 5.

Imidlertid ville det være ønskeligt, om lovgiver tog mere grundlæggende stilling til den nye digitale kontekst for agentvirksomhed. Det er fortsat definitioner og eksempler fra Strafferetsplejeudvalgets mere end 30 år gamle Betænkning, der er retningsgivende for selve agentmetoden. Eksempelvis nævnes i Bet. 1023/1984 den situation, hvor en civilklædt politimand på gaden tilfældigt forespørges af en forbipasserende, om han er interesseret i at købe hash, hvorefter politimanden viser interesse og følger med for at få forevist hashen med det formål at afsløre den pågældende som hashhandler.[306] En sådan situation vil ifølge Betænkningen ikke være omfattet af agentreglerne, idet situationen ikke er opstået på politimandens initiativ (jf. første led om at "tilbyde bistand"), ligesom der heller ikke er tale om et tilrettelagt arrangement, når situationen er tilfældigt opstået (jf. andet led om at "træffe foranstaltninger").[307] Spørgsmålet, som der i en digital kontekst må tages stilling til, er, om der på internettets platforme, hvor politiet optræder under dække, også er mulighed for, at disse kan blive tilfældigt kontaktede af mistænkte, med den konsekvens, at man er uden for agentreglernes anvendelsesområde. I så fald, hvor tilfældigt kan denne kontakt siges at være, hvis politiagenten først ved infiltration har formået at skaffe sig adgang til en privat gruppe, hvor en privat kommunikation kan følges i realtid. Politiets mere proaktive indsats på digitale platforme rummer således adskillige nye, retlige aspekter i relation til infiltration og agentvirksomhed.[308]

4.2. Internationalt samarbejde

Som det fremgik af Artikel 6: *"Politiagenter i et menneskeretligt perspektiv"*, pkt. 10, er det i to nyere danske sager sket, at domstolene måtte forholde sig til, at de lande, dansk politi samarbejder med, har andre retlige standarder for agentvirksomhed.

---

[305] Lene Wacher Lentz: "Hemmelig ransagning og brevstandsning i den digitale virkelighed", Juristen nr. 1/2016, s. 4 f.

[306] Bet. 1023/1984, s. 158.

[307] Bet. 1023/1984, s. 158.

[308] Jf. Artikel 5: *"Politiets infiltration på digitale platforme – set i et menneskeretligt perspektiv."*

Således var der i både U 2014.1080 H og U 2018.1169 H (den amerikanske civilagent) tale om amerikanske agentaktioner, der 'fortsatte' i Danmark. I begge tilfælde havde den involverede amerikanske agent foregivet at have tilknytning til FARC,[309] en colombiansk narkotika-relateret organisation, der på daværende tidspunkt var på EU's terrorliste.[310] I U 2014.1080 H havde agenten tilkendegivet, at han kunne skaffe kokain mod at få tunge militære våben i betaling, og at disse våben skulle bruges til en FARC-operation.[311] I U 2018.1169 H forklarede den amerikanske civilagent 'Maria', at han af sine overordnede havde fået at vide, at han overfor de tiltalte skulle foregive, at han var fra FARC, og at han var i stand til at levere og transportere 500 kg kokain til København.[312]

En sådan fremgangsmåde, hvor den agent, der handler på vegne af politi og myndigheder, hævder at være tilknyttet en terrororganisation, vil være ganske fremmed efter danske forhold, og ved vurderingen af sådanne agentaktioner må opmærksomheden særligt rettes mod, om der allerede som følge af denne (urigtige) tilkendegivelse kan ligge en pression eller en forøgelse af forbrydelsens karakter eller omfang. Ligeledes brugen af tidligere kriminelle som civilagenter, der har den centrale rolle i forløbet, som det var tilfældet med den amerikanske agent 'Maria' i U 2018.1169 H, må skærpe fokus på aktionens berettigelse og forløb.

De retlige standarder for disse internationale agentaktioner må først og fremmest bero på EMRK artikel 6, stk. 1 og Domstolens praksis i tilknytning hertil. Særligt må sikres oplysninger om det indledende mistankegrundlag for overhovedet at iværksætte agentaktionen over for de mistænkte, jf. Artikel 6: *"Politiagenter i et menneskeretligt perspektiv"*, pkt. 4.1. Dertil må aktionen overholde den danske regulering i retsplejelovens § 754 a ff. For så vidt angår agentaktioner relateret til internettet og de digitale platforme, kan disse også ske at finde sted i et større internationalt samarbejde, hvor det samme gør sig gældende.[313] I dette internationale, digitale samarbejde med 'undercover' politiaktioner vil der være adskillige juridiske aspekter at forholde sig til, herunder den straffeprocessuelle jurisdiktion, der handler om, hvilket lands regulering, der gælder for en sådan aktion. Hvis dansk politi deltager i

[309] "Fuerzas Armadas Revolucionarias de Colombia – Ejército del Pueblo" (Colombias revolutionære væbnede styrker – Folkets hær), jf. Wikipedia.
[310] FARC er blandt andet kendt for at have holdt den colombianske politiker, Íngrid Betancourt, som gidsel i junglen i over seks år. Efter indgåelse af en fredsaftale i 2016 med de colombianske myndigheder blev organisationen fjernet fra EU's terrorliste.
[311] Jf. hændelsesforløbet beskrevet i byrettens begrundelse, Ugeskriftet, s. 1087.
[312] Jf. hændelsesforløbet beskrevet i byrettens begrundelse, Ugeskriftet, s. 1173.
[313] Europarådets Cybercrimekonvention forholder sig ikke til sådanne aktioner, se hertil Inger Marie Sunde: "Cybercrime Law", i *"Digital Forensics"*, af André Årnes (ed.), 2018, s. 98.

internationale aktioner, må det forudsættes at ske efter retsplejelovens regulering, hvor bl.a. kravet om retskendelse må iagttages.

5. Opfølgning på begrebet det 'menneskelige indgreb'

Indledningsvist i afhandlingen blev der redegjort for betegnelsen 'det menneskelige indgreb', som måske kunne virke terminologisk distraherende i forhold til Hans Gammeltoft-Hansen traditionelle definition af et "tvangsindgreb", hvor politiets interageren med og påvirkning af borgeren netop ikke kunne betragtes som et indgreb.[314]

På baggrund af denne afhandlings analyse af de tre efterforskningsmetoder, infiltration, lokkedue og agentvirksomhed, forekommer betegnelsen 'menneskelige indgreb' for de tre metoder faktisk både dækkende og berettiget. Dette beror på den menneskeretlige forståelse af et 'indgreb' i privatliv, kommunikation m.v., jf. artikel 8, stk. 2, hvor EMD har anlagt en bredere forståelse af et indgreb, end det følger af Hans Gammeltoft-Hansens definition. Eksempelvis ses, at EMD betragter indsamling og registrering af oplysninger som indgreb i privatlivet, ligesom der kan gøres indgreb i retten til selvbestemmelse mv., jf. Artikel 5: *"Politiets infiltration på digitale platforme – set i et menneskeretligt perspektiv"*.

I forhold til politiets agentvirksomhed ses, at EMD som følge af *Lüdi*-sagen og efterfølgende praksis, anskuer sådanne sager i forhold til EMRK artikel 6, stk. 1 om retfærdig rettergang. Som det argumenteres i Artikel 5: *"Politiets infiltration på digitale platforme – set i et menneskeretligt perspektiv"*, er der ret beset to dele, som EMD kan forholde sig til i en agentaktion: Først selve bevisoptagelsen, som kan være infiltration, overvågning, påvirkning af borgeren og dennes selvbestemmelsesret, som rettelig er en artikel 8-problematik. Dernæst brugen af beviserne fra agentaktionen i en strafforfølgning mod borgeren, hvilket realiserer en artikel 6, stk. 1-vurdering. I det lys forekommer det berettiget at anvende betegnelsen 'det menneskelige indgreb' for efterforskningsmetoderne, infiltration, lokkeduesituationen og agentvirksomhed.

For disse tre efterforskningsmetoder – hvor infiltration selvsagt er den mildeste og for borgeren mindst indgribende metode – gælder, at borgeren i et vist omfang føres bag lyset, og at dette kan få betydning for en række af de beskyttede rettigheder i EMRK artikel 8, om privatliv, kommunikation, ret til selvbestemmelse og ret til at søge venskaber mv. Derudover kan også aspekter realiseres i forhold til EMRK artikel 6, således beskyttelse mod selvinkriminering, hvis der iscenesættes en form for afhørings-situation, foruden beskyttelse mod at politiet provokerer borgeren til en forbrydelse, der ellers ikke ville være blevet begået. Disse tre metoder kan efterforskningsmæssigt være overordentligt virkningsfulde. Blot må man ikke glemme, at helt

[314] Del 1, Kapitel 2, afsnit 3.2.

grundlæggende etiske aspekter bringes i spil, således politiets integritet, når borgeren på denne måde skal 'manipuleres', samt borgerens tillid til politiet som garant for tryghed, ordentlighed og sikkerhed i samfundet.

6. Sammenfatning vedrørende politiets 'menneskelige indgreb' på internettet

Til forskningsspørgsmålet om, hvordan reguleringen er af politiets 'menneskelige indgreb' på internettet, kan her anføres, at der er tale om to ulovregulerede metoder, infiltration og lokkedue-metoden, foruden agentvirksomhed, som er underlagt ganske restriktive betingelser om retskendelse og et kriminalitetskrav på 6 års fængsel eller derover, jf. retsplejelovens § 754 a ff. Grundstrukturen i denne regulering, der beror på 1984-Betænkningens definitioner og overvejelser, har ikke siden været genstand for en nyovervejelse i lyset af den nye kontekst af digitale platforme, nyere dansk retspraksis eller praksis fra EMD.

Der argumenteres retspolitisk for, at infiltration reguleres i lyset af EMRK artikel 8, stk. 2, jf. Artikel 5: *"Politiets infiltration på digitale platforme – set i et menneskeretligt perspektiv",* ligesom der argumenteres for en mere nuanceret tilgang til lokkedue-situationen, som i nogle tilfælde vil være at betragte som en uproblematisk iscenesat anholdelse, i andre tilfælde indeholde længerevarende kommunikation, påvirkning og et fristelsesmoment, der gør metoden sammenlignelig med agentvirksomhed, hvilket Lasse Lund Madsen har påpeget i relation til politiagenter på pædofile netværk.

Desuden argumenteres for at genoverveje den processuelle ramme for agentvirksomhed, hvor der konkret er peget på tiltag som advokatbeskikkelse og begrænsning i varigheden for at styrke den retlige vurdering af iværksættelse af agentvirksomhed og opfølgning på aktionens forsatte berettigelse.

I relation til samspillet mellem politiets tekniske indgreb og det 'menneskelige indgreb' er navnlig to forhold at bemærke: Først at infiltration i visse tilfælde vil kunne anskues som adgang på urigtige forudsætninger til private, lukkede systemer, hvorved infiltration får karakter af en sofistikeret 'hacking'-metode, jf. Artikel 5: "*Politiets infiltration på digitale platforme – set i et menneskeretligt perspektiv.*" Set i det lys, er det uholdbart, at infiltration er ulovreguleret, mens de tekniske indgreb, hemmelig ransagning, dataaflæsning mv. er underlagt restriktive betingelser om kriminalitetskrav, retskendelse, beskikkelse af indgrebsadvokat mv.

Dernæst er der om samspillet mellem det tekniske og det 'menneskelige indgreb' at bemærke, at der kan være behov for en hjemmel til 'digital observation' i det tilfælde, hvor politiet har fået adgang til et privat/lukket/beskyttet datasystem og ønsker at anvende software til at 'udvinde' oplysninger. I de tilfælde hvor adgangen er

sket ved et teknisk indgreb, hemmelig ransagning eller dataaflæsning, kan der i retskendelsen tillige tages stilling til, hvad politiet må foretage sig inde i systemet med det software og teknologi, man har til rådighed. Men der mangler en regulering af en sådan teknologisk 'dataudvinding' i de tilfælde hvor adgangen til det lukkede/private område er sket ved infiltration. I fravær af en sådan regulering må det formentlig have formodningen imod sig, at politiet efter ved infiltration at have fået adgang til et lukket/privat område måtte anvende teknologi til en større 'dataudvinding'. Situationen kunne løses enten ved en regulering af infiltrationen som en 'hacking'-metode på lige fod med den tekniske 'hacking', eller at der skabes en decideret hjemmel til denne teknologiske 'dataudvinding', som en form for digital observation med tekniske hjælpemidler.

Del 4 – Afslutning

Kapitel 1 Sammenfatning og perspektivering

1. Sammenfatning af de retspolitiske overvejelser

Denne afhandling har behandlet den retlige regulering af politiets efterforskning på internettet, hvor to typetilfælde er udvalgt: Politiets tekniske indgreb til at skaffe sig hemmelig adgang til internettets datasystemer mv., og politiets 'menneskelige indgreb', hvor politiet under dække interagerer med borgeren på internettet. I den retsdogmatiske analyse er påpeget flere problemfelter i den nugældende regulering, hvilket undervejs har givet anledning til en række retspolitiske overvejelser. I visse tilfælde har disse overvejelser udmøntet sig i en opfordring til mere konkrete tiltag, som sammenfattes i det følgende:

- En indsnævring af 'hacking'-bestemmelsens anvendelsesområde, navnlig i forhold til 'hacking' på de sociale medier.
- Overvejelser om, hvordan Tele2-sagen får indflydelse på den danske logningspligt og retsplejelovens regulering af politiets indgreb i meddelelseshemmeligheden.
- Reparation af et uheldigt samspil mellem de tre tekniske indgrebshjemler, hemmelig ransagning, dataaflæsning og indgreb i meddelelseshemmeligheden, i lyset af U 2012.2614 H, og en opfordring til at overveje en egentlig 'hacking'-hjemmel, der inddrager aspekter om kryptering og digital observation.
- Regulering af politiets mulighed for fremadrettet onlineovervågning ud fra beslaglagte mobiltelefoner.
- Regulering af det 'menneskelige indgreb', infiltration, som følge af EMRK, og af samme grund en genovervejelse af lokkedue-metoden.
- Styrkelse af den processuelle ramme om agentvirksomhed, herunder ved advokatbeskikkelse, og indførelse af en tidsfrist for aktionen, i lyset af dels nyere dansk retspraksis om agentvirksomhed, dels retspraksis fra EMD, der har forholdt sig restriktivt til politiets gentagne eller fortløbende agentaktioner.

De nye, forskelligartede, digitale efterforskningsmetoder har også givet anledning til en nyovervejelse af det straffeprocessuelle legalitetsprincip, hvor det fastlægges hvilke af politiets efterforskningsmetoder, der skal reguleres i retsplejeloven. Afhandlingens konklusion er, at man i højere grad må frigøre sig fra Hans Gammeltoft-Hansens definition af et tvangsindgreb, som målestokken for, hvornår regulering er nødvendig. I stedet må anlægges en konkret vurdering med løbende opfølgning på nye teknologiske efterforskningsmuligheder, samt dansk og menneskeretlig retspraksis. Domstolene får kun i begrænset omfang mulighed for at tage stilling til nye teknologiske metoder, og af hensyn til retssikkerheden og den samlede retsudvikling

på dette område, må lovgiver i højere grad være på forkant og foretage disse vigtige afvejninger mellem hensynet til strafforfølgning over for hensynet til de berørte borgere.

På baggrund af afhandlingens konklusioner gives i det følgende en perspektivering ud fra juridiske, men også friere og mere samfundsmæssige, overvejelser, om nogle af de overordnede, gennemgående temaer i afhandlingen.

2. Digitale udfordringer

Afhandlingens tema om politiets efterforskningsmuligheder på internettet illustrerer de tekniske, juridiske og kulturelle udfordringer, som strafferetten og straffeprocessen møder i den nye digitale kontekst. Det udsnit, der er lavet i denne afhandling, er blot en lille del af det samlede billede.

For så vidt angår den materielle strafferet er det i relation til 'hacking'-bestemmelsen påpeget, at der er flydende grænser mellem offentligt og privat område, og at der endnu ikke er etableret nogen egentlige digitale normer som 'sikker grund' for den strafferetlige regulering. Disse to aspekter gør sig også gældende for en række andre straffelovsbestemmelser, eksempelvis i forhold til deling af krænkende eller private billeder uden samtykke, jf. straffelovens § 264 d, hvor navnlig Umbrella-sagen med straffesager mod over 1000 personer for deling af en krænkende video satte fokus på samtykke, videredeling og digital opførsel generelt. I samme retning deling af Marokko-videoen med en sekvens af en henrettelse af en dansk kvindelig turist. Ligeledes i forhold til ytringer, hvor til tider ganske ophedede diskussioner på de sociale medier, foruden 'likes', delinger af indhold mv., kan realisere en række forskelligartede forbrydelser, således trusler, jf. straffelovens § 266, billigelse af terror, jf. § 136, stk. 2. Derudover kan brug og eksponering af personoplysninger realisere en overtrædelse af databeskyttelseslovgivningen.

I forhold til at beskytte det digitale privatliv er der en lang række yderligere aspekter at forholde sig til i de kommende år, hvor øget brug af offentligt tilgængelige oplysninger ("open source") giver mulighed for samkøring ("datamining"), hvorved der kan udledes ganske præcise data om os.[315] Dertil kommer de særlige overvågningstiltag i relation til nummerplader, flypassageroplysninger, teledata, videoovervåg-

[315] Om 'datamining', se Steen Manniche: "Er data neutralt?" i "*Ret SMART – om smart teknologi og regulering*", af Anita Rønne og Henrik Stevnsborg (red.), 2018, s. 35 f., og Lilian Edwards og Lachlan Urquhart: "Privacy in Public Spaces: What Expectations of Privacy Do We Have in Social Media Intelligence?" (December 11, 2015). International Journal of Law and Information Technology (Autumn 2016) 24 (3), 279-310.

ning i gadebilledet etc. Som borgere udsættes vi for mere offentlighed og transparens.[316] Netop denne overvågning og følelsen af konstant at være overvåget indgik som en central del af EU-Domstolens begrundelse i Tele 2-sagen. At finde balancepunktet mellem samfundets interesse i overvågning over for den enkeltes frihed bliver en konstant udfordring fremover.

Kriminalitetsbilledet, man ser på internettet, dækker et meget bredt spektrum, fra små og store økonomiske bedragerier og 'hacking'-angreb, salg af narkotika, hælervarer mv., samt forskellige former for ytringskriminalitet og privatlivskrænkelser mv. Der er dog ingen tvivl om, at den største og vigtigste udfordring skyldes de faciliteter, internettets anonyme, internationale platforme har givet for seksuelle krænkelser mod børn: 'Grooming' hvor der skabes kontakt til børn, der lokkes eller presses til forskellige seksuelle forhold, deling af billedmateriale med seksuelle krænkelser mod børn, samt bestilling over internettet af seksuelle overgreb mod børn, udført i andre lande og transmitteret i realtid via 'darkweb'.[317] I det fremtidige kriminalitetsbillede må sikres, at politiet har de fornødne, straffeprocessuelle rammer til at bekæmpe den alvorligste kriminalitet, terrorisme, overgreb mod børn, organiseret kriminalitet mv. Samtidig må det dog erkendes, at disse meget indgribende metoder ikke kan anvendes overalt og til efterforskning af alle former for kriminalitet, prisen er for høj i forhold til indskrænkningen af privatlivet, og den enkeltes frihed. Balancegangen er svær, men er ikke desto mindre nødvendig.

Den alvorligste digitale kriminalitet er i vidt omfang international, og strafferetten og straffeprocessen er voldsomt udfordret af, at de kriminelle har frit spil til at bevæge sig på internettet, mens de nationale politimyndigheder må respektere staternes selvbestemmelsesret. Dette betyder, at der skal anmodes om retshjælp landene imellem, når efterforskningen bevæger sig 'ind i' et andet land, eller bare igennem en server, hjemmehørende i et andet land. Denne tidskrævende proces er en udfordring, som der kun findes internationale løsninger på.

3. Teknologineutralitet som aspekt ved fremtidige reguleringer

Fra andre retsområder spiller princippet om teknologineutralitet en central rolle. Teknologineutralitet indebærer, at lovgivningen så vidt udformes neutralt i forhold til, hvilken teknik, der anvendes. Princippet om teknologineutralitet er vokset frem i takt med digitaliseringen af samfundet og reguleringen af forskellige digitale processer. Inden for databeskyttelsesreguleringen er det helt bevidst og meget karakteri-

[316] Jf. Peter Blume og Janne Rothmar Herrmann: "Se mig på nettet", Juristen nr. 4/2010.

[317] Se særligt om disse forbrydelser, Trine Vendius Thygesen: *"Europol & cyberkriminalitet – proaktiv efterforskning og forbrydelser mod børn"*, 2015.

stisk for retsområdet, at den nye Persondataforordning ikke nævner bestemte teknologier.[318] Således fremgår det af Forordningens præambel 15 i den danske oversættelse: "*For at undgå at skabe en alvorlig risiko for omgåelse bør beskyttelsen af fysiske personer være teknologineutral og ikke afhænge af de anvendte teknikker. Beskyttelsen af fysiske personer bør gælde for både automatisk og manuel behandling af personoplysninger, hvis personoplysningerne er indeholdt eller vil blive indeholdt i et register. Sagsmapper eller samlinger af sagsmapper samt deres forsider, som ikke er struktureret efter bestemte kriterier, bør ikke være omfattet af denne forordnings anvendelsesområde*."[319] Også indenfor eksempelvis teleretten spiller princippet om teknologineutralitet en rolle, hvoraf følger, at telelovgivningens regler skal anvendes ens, uanset hvilken for teknisk teleinfrastruktur, der er tale om, og bestemmelserne være tilstrækkeligt bredt formuleret til at kunne rumme nye former for netværk og tjenester, som løbende udvikles.[320]

I forhold til strafferetten kan det konstateres, at størstedelen af straffelovens traditionelle bestemmelser om drab, legemsangreb mv. i vidt omfang er beskrevet i forhold til den skade eller krænkelse, som forurettede eller samfundet oplever, og således uafhængigt af den 'metode', der forårsager drabet mv. På den måde kan en stor del af strafferetten for så vidt siges at være "teknologineutral."[321] Hverken inden for strafferetten eller straffeprocessen har der imidlertid været tale om en egentlig begrebsdannelse i forhold til princippet om teknologineutralitet, bortset fra enkelte tilkendegivelser om den teknologiske udvikling, eksempelvis i Brydensholt-udvalgets Bet. 1417/2002 om økonomisk kriminalitet og datakriminalitet, pkt. 2.6., hvor Udvalget i tilknytning til straffelovens § 1 om analogi anførte: "*Udvalget er opmærksom på, at dette krav om klar lovhjemmel om nødvendigt må gå forud for ønsket om en lovgivning, der er fremtidstilpasset til den mulige teknologiske udvikling, og at man i*

---

[318] Europa-Parlamentets og Rådets Forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse), se hertil bl.a. Peter Blume: "Databeskyttelse i den smarte verden" i "*Ret SMART – om smart teknologi og regulering"*, af Anita Rønne og Henrik Stevnsborg (red.), 2018, s. 40 ff.

[319] Forordningen fremgår som bilag 1 til den danske databeskyttelseslov, lov nr. 502 af 23. maj 2018.

[320] Se telelovens § 2, om definitioner og anvendelsesområde (lovbekendtgørelse nr. 128 af 7. februar 2014 om elektroniske kommunikationsnet og -tjenester), se hertil Søren Sandfeld Jakobsen (red.), Søren Johansen og Christian Bergqvist: "*Teleretten*", 2014, navnlig s. 72. Det ses endvidere af Justitsministeriets Vejledning om lovkvalitet, 2018, pkt. 4.3. om "Agil erhvervsrettet regulering", at der ved ny lovgivning generelt skal lægges vægt på, om reguleringen er teknologineutral, således at det understøttes, at virksomhederne kan følge med i den teknologiske udvikling.

[321] Inger Marie Sunde: "*Automatisert inndragning*", 2010, s. 115.

videst mulige omfang må forsøge at nå frem til formuleringer, der tilgodeser begge hensyn."

Udover at princippet om teknologineutralitet er relevant for lovgiver at tage i betragtning ved udarbejdelse af ny regulering, kan princippet også være relevant for retsanvendere, navnlig domstolene. Teknologineutralitet kan i den sammenhæng anskues som en fortolkningsmåde, således at forskellige teknologier ligestilles, hvis funktionaliteten i forhold til lovens kriterium er den samme.[322] I en sådan sammenhæng kan teknologineutralitet siges at være udtryk for den analogiske fortolkning, der kan foretages i forhold til en lovbestemmelses anvendelsesområde.

Selv om teknologineutralitet i strafferetten og straffeprocessen kan være en fordel, idet reguleringen eller retstilstanden derved 'teknologisk fremtidssikres', vil det samtidig være retssikkerhedsmæssigt betænkeligt, hvis retstilstanden derved kommer til at bero på *for* brede og abstrakte begreber i straffebestemmelser og straffeprocessuelle indgrebshjemler. Hvis det ikke angives, hvad der er henholdsvis det strafbare område i straffeloven og det tilladte indgreb for politiet, kan dette være problematisk i forhold til legalitetsprincippet. Således vil borgeren ikke vide, hvad der er strafbart efter straffeloven, og politiet vil stå med vanskelige kvalificeringer af de nye teknologiske muligheder, som lovgiver ikke har taget stilling til.

Teknologineutralitet kan også ses i den variant, at der så vidt muligt skal være overensstemmelse mellem adfærd i den digitale verden med adfærden i den velkendte fysiske verden, hvilket Sunde med citat fra Bert-Jaap Koops Koops gengiver som "what holds offline should also hold online."[323] Herved synes dog ikke længere at være tale om et rent lovteknisk hensyn eller fortolkningsmåde, men hensynet tilføres her en mere politisk og værdiladet dimension, som afhænger af, hvorvidt man egentlig er fortaler for, at den digitale verden fuldstændig skal afspejle den fysiske verden.

På dette sted i afhandlingen skal ikke følge en nærmere udredning og fastlæggelse af princippet om teknologineutralitet i forhold til dansk strafferet og straffeproces, men der synes bestemt at være et perspektiv i at inddrage og videreudvikle dette princip i den danske terminologi, som et princip både lovgiver og retsanvendere må forholde sig til og vurdere fordele og ulemper ved, når retstilstanden på nye digitale områder skal fastlægges.

---

[322] Inger Marie Sunde: "*Automatisert inndragning*", 2010, s. 115.

[323] Inger Marie Sunde: "*Automatisert inndragning*", 2010, s. 129 f. og 133, med henvisning til Bert Jaap Koops: "Should ICT Regulation Be Technology-Neutral?" in "*Starting Points for ICT Regulation. Deconstructing Prevalent Policy One-Liners*", IT & LAW SERIES, Bert-Jaap Koops, Miriam Lips, Corien Prins & Maurice Schellekens, eds., Vol. 9, pp. 77-108, The Hague: T.M.C. Asser Press, 2006.

I relation til denne afhandlings tema om 'hacking' efter straffelovens § 263 kan det konstateres, at både de tidligere begreber "anlæg til elektronisk databehandling" og "informationssystem", samt det nugældende begreb "datasystem" forekommer meget brede og derfor forholdsvis teknologineutrale, når deri omfattes stort set alt elektronisk, der indgår i eller kan kobles til en computer, således omfattes både usb-stik, servere, men også virksomheders intranet, profiler på sociale medier og måske også lukkede grupper på digitale platforme.[324]

I en straffeprocessuel kontekst kan det om en anden af denne afhandlings temaer, dataaflæsning, konstateres, at efterforskningsmetoden, som indebærer "Aflæsning af ikke offentligt tilgængelige oplysninger i et informationssystem ved hjælp af programmer eller andet udstyr", jf. retsplejelovens § 791 b, ikke har fået et bredt, teknologineutralt anvendelsesområde. Uden at Højesteret i kendelsen, U 2012.2614 H, nærmere har taget stilling til dataaflæsningens "programmer eller andet udstyr" i den kontekst, som internettet udgør, må retstilstanden være, at denne ordlyd må tages ret bogstaveligt, idet den almindelige hjemmel til politiets 'hacking' nu ses at være etableret som hemmelig ransagning.[325]

For disse to temaer vil konklusionen – lidt polemisk sagt – være, at straffelovens 'hacking'-bestemmelse med sit meget brede anvendelsesområde bærer præg af "for meget teknologineutralitet", mens retsplejelovens dataaflæsningsindgreb har fået et meget smalt anvendelsesområde og derfor indeholder "for lidt teknologineutralitet".

Til inspiration for hvordan teknologineutralitet som princip i dansk strafferet og straffeproces kan videreudvikles, kan blikket i første omgang rettes mod norsk ret, hvor man eksempelvis har forholdt sig udtrykkeligt til princippet om teknologineutralitet i "Ny straffeprosesslov", Utredning fra Straffeprosessutvalget, afgivet til Justis- og beredskapsdepartementet den 3. november 2016 (NOU 2016:24). Her fylder teknologineutralitet ganske meget, således i det indledende pkt. 6.1.: *"Lovutkastet er imidlertid så langt det har latt seg gjøre utformet teknologinøytralt. [ ]. I en del tilfeller der det ellers knytter seg særlige spørgsmål til håndtering eller bruk av teknologi, er dette drøftet særskilt i tilknytning til de enkelte bestemmelser i utkastet."*[326]

[324] Jf. Artikel 1: "*'Hacking' og det digitale privatliv*."
[325] Jf. Artikel 4: "*Politiets hjemmel til 'hacking' som led i en efterforskning*", pkt. 3.2.
[326] Se endvidere NOU 2016:24, pkt. 6.2.3.

Som det ses indgår begrebet teknologineutralitet i lovgivningsprocessen som en bevidsthed om teknologiens betydning og udfordring for lovteksten, forståelsen heraf og den fremtidige retsudvikling.[327]

4. Dansk straffeproces og internationale strømninger

Dansk straffeproces har igennem årene levet forholdsvis isoleret fra international ret, idet Hans Gammeltoft-Hansens definition af et straffeprocessuelt indgreb har været den målestok for regulering, som lovgiver og domstolene i vidt omfang har taget udgangspunkt i og forholdt sig til. Påvirkningen fra EU er dog stigende, og uanset det danske retsforbehold kommer EU-samarbejdet til at få øget indflydelse på dansk straffeproces fremover. Dette ses eksempelvis i afhandlingens tema om logning, hvor EMD's udtalelser i Tele2-sagen får betydning for de danske regler om indgreb i meddelelseshemmeligheden. Ligeledes ses en øget påvirkning fra EMD, som i sin praksis udvikler nye konkrete og detaljerede anvisninger i sin fortolkning af Konventionens rettigheder.

Den danske tilgang til nye initiativer fra EU og retsudviklingen fra EMD, både i forhold til den materielle strafferet og i forhold til straffeprocessen, synes at være forholdsvis 'minimalistisk', jf. Pernille Boye Kochs terminologi.[328] Således ses i denne afhandlings tema om 'hacking', at lovgivers stillingtagen til EU's Cybercrimedirektiv beror på, om det er nødvendigt at ændre noget, eller om den danske retstilstand kan rummes inden for Cybercrimedirektivets ramme, ikke om der er inspiration at hente fra nye tiltag i EU-regi. Navnlig i relation til IT-kriminalitet og efterforskningen heraf, står de vestlige lande med samme problemer, og hvad der er udfordringer og løsninger i andre i lande, kunne også være relevant for Danmark. Om den danske tilgang skal kaldes minimalistisk, eller måske ligefrem defensiv, vil i realiteten være udtryk for det samme, nemlig et nationalt perspektiv for strafferet og straffeproces, hvor nye internationale tiltag i vidt omfang ses som en indgriben heri. Debatten kommer let til at handle om suverænitetsafgivelse og national selvbestemmelse, i stedet for det indholdsmæssige udbytte. Europol-afstemningen, som drejede sig om tilvalg af mange interessante retsakter og initiativer i EU-regi, kan ses som en illustration af dette.

Trine Baumbach har talt om dansk 'ambivalens' mellem strafferetten og EU-retten, med henvisning til, at Danmark i vidt omfang bringer sin straffelovgivning i overensstemmelse med de retsakter, som de andre EU-medlemslande har vedtaget, og at

---

[327] Se endvidere om teknologineutralitet, Jul Fredrik Kaltenborn: "Teknologinøytralitet og datakriminalitet – særlig om klassifiseringen av begrebet datasystem", Tidsskrift for Strafferett, nr. 2-2019, s. 148-167.

[328] Pernille Boye Koch: "Lovgivers rolle som fortolker af internationale retskilder – på hvilken måde gælder menneskerettighederne i Danmark?", Tidsskrift for Rettsvitenskap, vol. 132, 1/2019, s. 3-50.

Danmark tilsyneladende gerne vil 'fuldintegreres', samtidig med at Danmark som følge af retsforbeholdet har *"iklædt sig en fodlænke, der ikke er lang nok til, at Danmark beslutningsmæssigt kan sidde med ved bordet."*[329]

Mens der således internationalt, i regi af EU og Europarådet i relation til Cybercrimekonventionen mv., gøres nye tiltag til øget samarbejde om fælles udfordringer til bekæmpelse af den internationale, grove og grænseoverskridende kriminalitet, er det også fra international side, at der sker en øget og mere detaljeret beskyttelse af den enkelte borgers rettigheder, eksemplificeret ved EU's databeskyttelsesregulering, Chartret om grundlæggende rettigheder og Europarådets Menneskerettighedskonvention.

5. Bevisvurdering og den materielle sandheds princip

I dansk straffeproces gælder et princip om fri bevisvurdering, jf. retsplejelovens § 880, hvoraf følger, at retten ved afgørelsen af, om noget er bevist eller ikke, alene tager hensyn til de beviser som er ført under hovedforhandlingen, og at rettens bedømmelse af bevisernes vægt ikke er bundet ved lovregler.[330]

Danske domstole har i udgangspunktet en forholdsvis pragmatisk tilgang til at tillade beviser ført, uanset der kan konstateres kritiske eller ulovlige forhold i forbindelse med bevisoptagelsen.[331] Hvorvidt beviser tillades ført, beror ifølge Birgitte Brøbech på en samlet vurdering, hvori indgår, om der alene er tale om en formel mangel, eller om de materielle betingelser for indgrebet ikke var opfyldt, samt hvorvidt beviset skønnes pålideligt, og hvorvidt beviset er af afgørende betydning for sagens udfald.[332] I bund og grund handler det om, at retten helst selv vil 'se' beviset, så man kan vurdere, om det skal have nogen betydning for straffesagen. Kun i sjældne tilfælde afskæres beviser, uden at retten får kendskab til indholdet heraf. Denne tilgang tilgodeser hensynet til princippet om at finde frem til den materielle sandhed, og at beviset trods alt kan have en værdi og sige noget om, hvad der er foregået.

---

[329] Baumbach: "Strafferetten og EU" i "*Retskildernes kamp – Forholdet mellem national offentlig ret og udefra kommende ret*" af Trine Baumbach og Peter Blume (red.), 2012, s. 69.

[330] Se hertil Michael Kistrup m.fl.: *"Straffeprocessen"*, 2018, s. 679 ff.

[331] Om domstolenes tilbageholdenhed med at afskære ulovligt tilvejebragte beviser, se Michael Kistrup m.fl. *"Straffeprocessen"*, 2018, s. 27 f. og 678 ff., samt Lene Wacher Lentz: "Efterforskningens grænser på internettet", i "*Eksponeret – Grænser for privatliv i en digital tid*", af Rikke Frank Jørgensen og Birgitte Kofod Olsen (red.), 2018, s. 139.

[332] Jf. Birgitte Brøbech: *"Ulovligt tilvejebragte beviser i straffeprocessen"*, 2003, s. 401 ff., som her refereret fra Lene Wacher Lentz: "Efterforskningens grænser på internettet", i "*Eksponeret – Grænser for privatliv i en digital tid*", Rikke Frank Jørgensen og Birgitte Kofod Olsen, 2018, s. 150, note 3.

Mere overordnet set hviler den danske tilgang på en høj grad af tillid til, at dansk politi og myndigheder generelt ikke misbruger magtbeføjelserne, og at sådanne fejl kan håndteres med kritik af fremgangsmåder mv., og eventuelt med disciplinæransvar for de enkelte, der har været involveret i fejl og forsømmelser.

Praksis fra EMD støtter til en vis grad en sådan tilgang. Således ses det, at EMD i relation til beviser tilvejebragt i strid med retten til privatliv, korrespondance, jf. artikel 8, ikke finder, at brugen af sådanne beviser som (del af) grundlaget for en domfældelse automatisk krænker artikel 6, stk. 1 om retfærdig rettergang, jf. eksempelvis *Khan*-sagen, hvor en telefonaflytning ikke var i overensstemmelse med loven, hvilket indebar en krænkelse af EMRK artikel 8, men den efterfølgende brug af aflytningen som bevis mod Khan i en straffesag udgjorde ikke et brud på artikel 6, stk. 1.[333] Dog ses EMD ved beviseksklusionen i relation til agentaktioner i strid med artikel 6, stk. 1. på dette område at have anlagt en mere restriktiv linie.[334]

Såfremt der i stedet i dansk straffeproces herskede en mere formalistisk tilgang, hvor alle fejl og ulovligheder ved bevisoptagelsen automatisk ville resultere i bevisudelukkelse, ville tankegangen i stedet være, at det ikke skulle kunne betale sig for politiet at overtræde reglerne. Risikoen ved en sådan formalistisk tilgang vil være, at straffesagens fokus skifter fra det materielle indhold, hvem gjorde hvad og hvornår, til en minutiøs, juridisk fejlfinding af formalia omkring efterforskningen, hvis det er der, forsvaret bedst vurderer kræfterne brugt i forhold til at svække strafforfølgningen mod klienten. Alt andet lige vil konsekvensen af, at en straffesag afgøres ud fra formalia og bevisudelukkelse, være, at flere skyldige går fri.

I forhold til at få oplyst sagen og finde frem til den materielle sandhed er den danske, pragmatiske tilgang – indenfor rammerne af EMRK og EMD's praksis – at foretrække. Denne tilgang bygger på tillid til politiet og overholdelse af rammer for efterforskningen og respekten for borgerens privatliv, kommunikation mv. Hvis rammerne for politiet opleves at blive for løse, usammenhængende og skønsmæssigt overladt til den enkelte polititjenestemands overvejelser, således at der eksempelvis opleves udbredt politiovervågning på digitale platforme, tilfældige og usaglige indgreb, fæl-

[333] Jf. Artikel 5: *"Politiets infiltration på digitale platforme – set i et menneskeretligt perspektiv"*, pkt. 4.2., med henvisning til *Khan mod Storbritannien*, dom af 12. maj 2000, pkt. 26-40.
[334] Jf. Artikel 6: *"Politiagenter i et menneskeretligt perspektiv"*, pkt. 4.3. Om EMD's praksis for beviseksklusion, se Ana María Torres Chedraui: "An analysis of the exclusion of evidence obtained in violation of human rights in light of the jurisprudence of the European Court of Human Rights", Tilburg Law Review 2010, volume 15, issue 2.

der og fristelser for den enkelte mv., kan den grundlæggende tillid til politiet svækkes.[335] Af hensyn til et fortsat velfungerende straffesystem, som der hersker stor respekt om, er det afgørende til stadighed at sikre faste rammer for politiets efterforskning over for borgerens privatliv og frihed.

6. Tillid til politi og straffesystem

Talrige undersøgelser har gennem årene vist, at danskerne har meget høj tillid til politiet. Disse undersøgelser dækker over en lang række forskelligartede spørgsmål, hvor forståelsen og definitionen af begrebet "tillid" altid kan diskuteres. Ud fra Den Danske Værdiundersøgelse 2017 kan det konstateres, at omkring 90 % af de adspurgte havde svaret, at man havde meget stor eller ret stor tillid til politiet, og at dette havde været uændret siden 1981, jf. Bilag 2.

Samme billede ses i Politiets tryghedsundersøgelse, fra december 2019,[336] hvor det i pkt. 4 om tilliden til politiet fremgår, at fokuspersonerne er blevet spurgt, om de har tillid til, at politiet vil hjælpe dem, hvis de har brug for det. På landsplan viste undersøgelsen, at 83,5 procent af borgerne i Danmark havde tillid til politiet i 2018, og sammenlignet med 2013, hvor Rigspolitiet målte tilliden for første gang, er borgernes tillid til politiet uændret på landsplan.

Rapporten "Tryghed og holdning til politi og retssystem Danmark i forhold til andre europæiske lande", udgivet af Justitsministeriets Forskningskontor, januar 2016, er baseret på data bearbejdet fra en spørgeskemaundersøgelse, der er gennemført i 15 europæiske lande i 2014, *European Social Survey* (ESS).[337] Undersøgelsen fra 2014 viste bl.a. at Danmark lå på andenpladsen med hensyn til tillid til politiet, og at der fra 2012 til 2014 var sket et mindre fald i befolkningens tillid til politiet, men at Danmark igen lå i top med hensyn til tillid til retssystemet.

Den private virksomhed, PwC, lancerede i 2018 i samarbejde med Epinion et nyt Tillidsbarometer, hvor ca. 1.500 danskere svarede på spørgsmål om tillid til hinanden og omverdenen, herunder deres opfattelse af en række forskellige institutioner. Undersøgelsen viste, at politiet indtog førstepladsen som den institution, som danskerne havde mest tillid til.[338]

---

[335] Se om autoritet i politiprofessionen, herunder om politiets legitimitet, borgerens tillid til politiet og oplevelse af retfærdighed, Adam Diderichsen og Anne-Stina Sørensen (red.): *"Den skarpe ende. Grundbog i politiarbejde*", 2016, s. 181 ff.
[336] Tilgængelig på www.politi.dk
[337] Tilgængelig på www.jm.dk.
[338] Tilgængelig på www.pwc.dk

Uagtet dette overordnede positive billede ses dog også eksempler på områder med lav tillid til politiet, således fra dagspressen i maj 2019, hvor en Tryghedsmåling foretaget af Megafon baseret på 1019 respondenter viste, at kun én ud af 20 danskere troede på, at politiet ville opklare et indbrud i deres hjem.[339] Dette ændrer dog ikke på det overordnede, positive billede, men er et eksempel på, at borgernes erfaringer på konkrete områder af politiets arbejde kan rokke ved den udbredte tillid.

Tillid og opbakning til politiet er ikke uforanderlige størrelser, men skyldes årevis af optjent integritet og lovmæssighed, hvor indtrykket er, at der følges op på fejl og forsømmelser, og at brodne kar i styrken håndteres disciplinært eller strafferetligt. Ved at sikre, faste, overordnede, lovgivningsmæssige rammer for politiets efterforskningsmæssige værktøjer, navnlig i den nye, digitale æra, kan forudsætningerne skabes for, at politiets arbejde også fremover er præget af lovmæssighed, retssikkerhed, og dermed en udbredt tillid til straffesystemet.

[339] http://nyheder.tv2.dk/krimi/2019-05-21-ny-maaling-viser-meget-lav-tillid-til-politiet

Bilag

1. Brev til Facebook

Bilag

2. Uddrag af Den Danske Værdiundersøgelse

Bilag

3. Domsliste

Ugeskrift for Retsvæsen:

U 2019.2019 Ø
U 2019.1304 H
U 2018.1787 H
U 2018.1169 H
U 2018.993 V
U 2017.3544 Ø
U 2017.1689 Ø
U 2017.1243 H
U 2017.247 V
U 2016.3605 Ø
U 2016.2666 V
U 2016.351 Ø
U 2015.3615 Ø
U 2015.1525 H
U 2015.1249 H
U 2015.345 Ø
U 2014.1080 H
U 2013.3047/2 H
U 2013.2829 V
U 2012.2225 Ø
U 2012.2614 H
U 2012.1045 Ø
U 2011.399 Ø
U 2009.2610 H
U 2009.1109 Ø
U 2008.1734 V
U 2008.1094 V
U 2008.843 V
U 2008.671 H
U 2007.1673 Ø
U 2007.22 Ø
U 2005.777 V
U 2003.137 H
U 2002.2314 V
U 2002.1064 V
U 2002.340 H
U 2001.1276 H
U 2001.245 Ø
U 2000.2476 H
U 2000.1450 Ø
U 1999.985 H
U 1999.320 Ø
U 1999.178 V
U 1996.1496 V
U 1999.985 H
U 1999.320 Ø
U 1999.178 V
U 1998.1443 Ø
U 1998.800 H
U 1997.1021 H
U 1996.1496 V
U 1996.356 Ø
U 1995.374 H
U 1993.1 H
U 1992.638 V
U 1990.70/2 H
U 1970.680/1 V
U 1963.1031/2 V
U 1963.1029/1 V
U 1956.158 Ø
U 1940.156 Ø

Tidsskrift for Kriminalret:

TfK 2017.1034 Ø
TfK 2015.612 Ø
TfK 2008.416 V

Utrykt praksis:
Østre Landsrets ankedom af 7. marts 2017 (S-2696-16)
Østre Landsrets utrykte ankedom af 19. maj 2016 (S-1637-15)

Anklagemyndighedens Vidensbase:
AM2013.05.02B2

EMD-praksis:
Adamson mod Storbritannien, afgørelse af 26. januar 1999 (42293/98).

Allan mod Storbritannien, dom af 5. november 2002 (48539/99).

Amann mod Schweiz, dom af 16. februar 2000 (27798/95).

Association "21 December 1989" og andre mod Rumænien, dom af 24. maj 2011 (33810/07).

Austin og andre mod Storbritannien, dom af 15. marts 2012 (39692/09 m.fl.)

Bajsultanov mod Østrig, dom af 12. juni 2012 (54131/10).

Bannikova mod Rusland, dom af 4. november 2010 (18757/06).

Bărbulescu mod Rumænien, dom af 5. september 2017 (61496/08).

*Belgian Linguistic-sagen (*CASE "RELATING TO CERTAIN ASPECTS OF THE LAWS ON THE USE OF LANGUAGES IN EDUCATION IN BELGIUM" v. BELGIUM), dom af 23. juli 1968 (1474/62 m.fl.)

Benet Czech, Spol, S.R.O. mod Tjekkiet, dom af 21. oktober 2010 (31555/05).

Benet Praha, Spol. S.R.O. mod Tjekkiet, dom af 24. februar 2011 (33908/04 m.fl.)

Bensaid mod Storbritannien, dom af 6. februar 2001 (44599/98).

Botta mod Italien, dom af 24. februar 1998 (21439/93).

Bouchelkia mod Frankrig, dom af 29. januar 1997 (23078/93).

Burghartz mod Schweiz, dom af 22. februar 1994 (16213/90).

C mod Belgien, dom af 7. august 1996 (21794/93).

Calabrò mod Italien og Tyskland, dom af 21. marts 2002 (59895/00).

Camenzind mod Schweiz, dom af 16. december 1997 (21353/93).

Cantoni mod Frankrig, dom af 11. november 1996 (17862/91).

Catan og andre mod Moldova og Rusland, dom af 19. oktober 2012 (43370/04 m.fl.)

Cemalettin Canlı mod Tyrkiet, dom af 18. november 2008 (22427/04).

Coëme og andre mod Belgium, dom af 22. juni 2000 (32492/96 m.fl.)

Constantin og Stoian mod Rumænien, dom af 29. september 2009 (23782/06).

Copland mod Storbritannien, dom af 3. april 2007 (62617/00).

Custers, Deveaux og Turk mod Danmark, dom af 3 maj 2007 (11843/03 m.fl.)

Del Río Prada mod Spanien, dom af 21. oktober 2013 (42750/09).

Dragotoniu og Militaru-Pidhorni mod Rumænien, dom af 24. maj 2007 (77193/01 m.fl.)

El-Masri mod The Former Yugoslav Republic of Macedonia, dom af 13. december 2012 (39630/09).

Eurofinacom mod Frankrig, afgørelse af 7. september 2004 (58753/00).

Fernández Martínez mod Spanien, dom af 12. juni 2014 (56030/07).

Frérot mod Frankrig, dom af 12. juni 2007 (70204/01).

Friedl mod Østrig, dom af 31. januar 1995 (15225/89).

Furcht mod Tyskland, dom af 23. oktober 2014 (54648/09).

Gillan and Quinton mod Storbritannien, dom af 12. januar 2010 (4158/05).

Grba mod Kroatien, dom af 23. november 2017 (47074/12).

Groppera Radio AG mod Schweiz, dom af 28. marts 1990 (10890/84).

H-Ł mod Polen, dom af 15. september 2015 (14781/07 m.fl.)

Handyside mod Storbritannien, dom af 7. december 1976 (5493/72).

Huhtamäki mod Finland, dom af 6. marts 2012 (54468/09).

I mod Finland, dom af 17. juli 2008 (20511/03).

Idalov mod Rusland, dom af 22. maj 2012 (5826/03).

Isaksson og andre mod Sverige, afgørelse af 8. marts 2016 (29688/09 m.fl.)

Ivashchenko mod Rusland, dom af 13. februar 2018 (61064/10).

Jorgic mod Tyskland, dom af 12. juli 2007 (74613/01).

K.-H. W. mod Tyskland, dom af 22. marts 2001 (37201/97).

Kafkaris mod Cypern, dom af 12. februar 2008 (21906/04).

Kennedy mod Storbritannien, dom af 18. maj 2010 (26839/05).

Khan mod Storbritannien, dom af 12. maj 2000 (35394/97).

Khudobin mod Rusland, dom af 26. oktober 2006 (59696/00).

Klass og andre mod Tyskland, dom af 6. september 1978 (5029/71).

Kokkinakis mod Grækenland, dom af 25. maj 1993 (14307/88).

Kroon og andre mod Holland, dom af 27. oktober 1994 (18535/91).

Kruslin mod Frankrig, dom af 24. april 1990 (11801/85).

Kudła mod Polen, dom af 26. oktober 2000 (30210/96).

Kuzmickaja mod Litauen, afgørelse af 10. juni 2008 (27968/03).

Lagutin og andre mod Rusland, dom af 24. april 2014 (6228/09 m.fl.)

Langner mod Tyskland, dom af 17. september 2015 (14464/11).

Laurent mod Frankrig, dom af 24. maj 2018 (28798/13).

Leander mod Sverige, dom af 26. marts 1987 (9248/81).

Liberty og andre mod Storbritannien, dom af 1. juli 2008 (58243/00).

Liivik mod Estland, dom af 25. juni 2009 (12157/05).

López Ribalda og andre mod Spanien, dom af 9. januar 2018, afventer Storkammerets dom (1874/13 m.fl.)

Lüdi mod Schweiz, dom af 15. juni 1992 (12433/86).

Malone mod Storbritannien, dom af 2. august 1984 (8691/79).

Marguš mod Kroatien, dom af 27. maj 2014 (4455/10).

Matanovic mod Kroatien, dom af 4. april 2017 (2742/12).

Mazurek mod Frankrig, dom af 1. februar 2000 (34406/97).

Michaud mod Frankrig, dom af 6. december 2012 (12323/11).

Milinienė mod Litauen, dom af 24. juni 2008 (74355/01).

Müller mod Østrig, afgørelse af 28. juni 1995 (22463/93).

Murray mod Storbritannien, dom af 28. oktober 1994 (14310/88).

Narinen mod Finland, dom af 1. juni 2004 (45027/98).

Navalnyye mod Rusland, dom af 17. oktober 2017 (101/15).

Niemitz mod Tyskland, dom af 16. december 1992 (13710/88).

Oleksandr Volkov mod Ukraine, dom af 9. januar 2013 (21722/11).

P.G. og J.H mod Storbritannien, dom af 25. september 2001 (44787/98).

Paradiso og Campanelli mod Italien, dom af 24. januar 2017 (25358/12).

Pătraşcu mod Rumænien, dom af 14. februar 2017 (7600/09).

Peck mod Storbritannien, dom af 28. januar 2003 (44647/98).

Perinçek mod Schweiz, dom af 15. oktober 2015 (27510/08).

Petri Sallinen og andre mod Finland, dom af 27. september 2005 (50882/99).

Piechowicz mod Polen, dom af 17. april 2012 (20071/07).

Pretty mod Storbritannien, dom af 29. april 2002 (2346/02).

Rajcoomar mod Storbritannien, afgørelse af 14. december 2004 (59457/00).

Ramanauskas mod Litauen, dom af 5. februar 2008 (74420/01).

Rohlena mod Tjekkiet, dom af 27. januar 2015 (59552/08).

Roman Zakharov mod Rusland, dom af 4. december 2015 (47143/06).

Rotaru mod Rumænien, dom af 4. maj 2000 (28341/95).

S.E. mod Schweiz, afgørelse af 4. marts 1998 (28994/95).

S.W. mod Storbritannien, dom af 22. november 1995 (20166/92).

Saadi mod Storbritannien, dom af 29. januar 2008 (13229/03).

Sanchez Cardenas mod Norge, dom af 4. oktober 2007 (12148/03).

Saunders mod Storbritannien, dom af 17. december 1996 (19187/91).

Scholer mod Tyskland, dom af 18. december 2014 (14212/10).

Segerstedt-Wiberg og andre mod Sverige, dom af 6. juni 2006 (62332/00).

Sequeira mod Portugal, afgørelse af 6. maj 2003 (73557/01).

Shannon mod Storbritannien, afgørelse af 6. april 2004 (67537/01).

Shimovolos mod Rusland, dom af 21. juni 2011 (30194/09).

Silver og andre mod Storbritannien, dom af 25. marts 1983 (5947/72 m.fl.)

Smirnova mod Rusland, dom af 24. juli 2003 (46133/99 m.fl.)

Société Colas Est og andre mod Frankrig, dom af 16. april 2002 (37971/97).

Soros mod Frankrig, dom af 6. oktober 2011 (50425/06).

Stec og andre mod Storbritannien, afgørelse af 6. juli 2005 (65731/01 m.fl.)

Streletz, Kessler and Krenz mod Tyskland, dom af 22. marts 2001 (34044/96 m.fl.)

Szabó og Vissy mod Ungarn, dom af 12. januar 2016 (37138/14).

Tchokhonelidze mod Georgien, dom af 28. juni 2018 (31536/07).

Teixeira de Castro mod Portugal, dom af 9. juni 1998 (25829/94).

Tyrer mod Storbritannien, dom af 25. april 1978 (5856/72).

Uzun mod Tyskland, dom af 2. september 2010 (35623/05).

Valenzuela Contreras mod Spanien, dom af 30. juli 1998 (27671/95).

Van der Heijden mod Holland, dom af 3. april 2012 (42857/05).

Van Kück mod Tyskland, dom af 12. juni 2003 (35968/97).

Vanyan mod Rusland, dom af 15. december 2005 (53203/99).

Veselov og andre mod Rusland, dom af 2. oktober 2012 (23200/10 m.fl.)

Vinter og andre mod Storbritannien, dom af 9. juli 2013 (66069/09 m.fl.)

Volkov og Adamskiy mod Rusland, dom af 26. marts 2015 (7614/09 m.fl.)

Weber og Saravia mod Tyskland, afgørelse af 29. juni 2006 (54934/00).

Wieser and Bicos Beteiligungen GmbH mod Østrig, dom af 16. oktober 2007 (74336/01).

X. mod Holland, afgørelse af 12. december 1977 (7721/76).

X. mod Storbritannien, afgørelse af 10. december 1975 (6683/74).

X. mod Østrig, afgørelse af 22. april 1965 (1852/63).

Z. mod Finland, dom af 25. februar 1997 (22009/93).

Bilag

4. Litteraturliste

Bøger:

Andersen, Mads Bryde: *"IT-retten"*, 2. udgave, 2005, Forlaget Gjellerup.

Andersen, Mads Bryde: *"Ret & Metode"*, 2002, Forlaget Gjellerup.

Andersen, Poul: "*Dansk forvaltningsret. Almindelige emner",* 5. udgave, 1965, Gyldendal.

Baumbach, Trine: "*Medieret – frihed og ansvar*", 1. udgave, 2017, Karnov Group.

Baumbach, Trine: *"Strafferet og menneskeret"*, 1. udgave, 2014, Karnov Group.

Baumbach, Trine: *"Det strafferetlige legalitetsprincip – hjemmel og fortolkning "*, 1. udgave 2008, Jurist- og Økonomforbundets Forlag.

Beling, Ernst: *"Die Lehre vom Verbrechen"*, Tübingen 1906.

Blume, Peter og Janne Rothmar Herrmann: *"Ret, privatliv og teknologi"*, 4. udgave, 2018, Jurist- og Økonomforbundets Forlag.

Blume, Peter: *"Retssystemet og juridisk metode"*, 3. udgave, 2016, Jurist- og Økonomforbundets Forlag.

Blume, Peter: *"Juridisk metodelære"*, 5. udgave, 2009, Jurist- og Økonomforbundets Forlag.

Blume, Peter, Kirsten Ketscher og Steen Rønsholdt (red.): "*Liv, arbejde og forvaltning*", 1995, GadJura.

Blume, Peter og Hanne Petersen (red.): "*Retlig polycentri*", 1993, Akademisk Forlag.

Bruce, Ingvild og Geir Sunde Haugland: *"Skjulte tvangsmidler"*, 2. utgave, 2018, Universitetsforlaget.

Brøbech, Birgitte: *"Ulovligt tilvejebragte beviser i straffeprocessen"*, 2003, Jurist- og Økonomforbundets Forlag.

Bønsing, Sten: *"Almindelig forvaltningsret"*, 4. udgave, 2018, Jurist- og Økonomforbundets Forlag.
Christensen, Malene Bechmann: "*Det strafferetlige samtykke*", 2008, Jurist- og Økonomforbundets Forlag.

Christoffersen, Jonas, Lasse Højlund Christensen, Lasse Lund Madsen, Louise Halleskov Storgaard, Henrik Skovgaard-Petersen, Maria Ventegodt: *"EU's Charter om Grundlæggende rettigheder med kommentarer"*, 2. udgave, 2018, Jurist- og Økonomforbundets Forlag.

Dalberg-Larsen, Jørgen: *"Rettens enhed – en illusion? Om retlig pluralisme i teorien og i praksis"*, 1994, Akademisk Forlag

Diderichsen, Adam og Anne-Stina Sørensen (red.): *"Den skarpe ende. Grundbog i politiarbejde*", 1. udgave, 2016, Samfundslitteratur.

Dijk, Peter van, Fried van Hoof, Arjen van Rijn and Leo Zwaak (eds.): *"Theory and Practice of the European Convention on Human Rights"*, Fourth Edition, 2006, Intersentia.

Elholm, Thomas, Morten Niels Jakobsen og Lasse Lund Madsen: "*Kommenteret straffelov Almindelig del*", 11. udgave, 2019, Jurist- og Økonomforbundets Forlag.
Evald, Jens og Sten Schaumburg-Müller: *"Retsfilosofi, retsvidenskab og retskildelære"*, 2004, Jurist- og Økonomforbundets Forlag.

Eyben, Bo von: "*Juridisk ordbog*", 14. udgave, 2016, Karnov Group.

Frände, Dan: *"Den straffrättsliga legalitetsprincippet"*, 1989, Ekenäs Tryckeri.
Gammeltoft-Hansen, Hans: *"Straffeprocessuelle tvangsindgreb"*, 1981, Jurist- og Økonomforbundets Forlag.

Greve, Emil Bock: *"Politiets efterretningstjeneste - En retlig belysning af tjenestens virksomhed og det samlede kontrolsystem"*, 1. udgave 2014, Jurist- og Økonomforbundets Forlag.

Greve, Vagn: *"Det strafferetlige ansvar"*, 2. udgave, 2004, Jurist- og Økonomforbundets Forlag.

Greve, Vagn, Poul Dahl Jensen og Gorm Toftegaard Nielsen: *"Kommenteret straffelov. Almindelig del*", 2013, Jurist- og Økonomforbundets Forlag.

Greve, Vagn, Asbjørn Jensen, Bent Unmack Larsen, Per Lindegaard og Gorm Toftegaard Nielsen: *"Kommenteret Straffelov, Speciel del"*, 5. omarbejdede udgave, 1994, Jurist- og Økonomforbundets Forlag.

Greve, Vagn: "*edb-strafferet*", 2. reviderede udgave, 1986, Jurist- og Økonomforbundets Forlag.

Guðmundsdóttir, Helena Lybæk: *"Clarifying broad hacking statutes"*, Ph.d.-afhandling, 2015, Aalborg Universitet.

Harhoff, Frederik (red.), Ulrike Barten, Kenneth Øhlenschlæger Buhl, Bugge Thorbjørn Daniel, Birgit Feldtmann, og Sten Schaumburg-Müller: *"Folkeret"*, 2017, Hans Reitzels Forlag.

Harris, D.J., M. O'Boyle, E. Bates og C. Buckley: *"Law of European Convention on Human Rights"*, 4th edition, 2018, Oxford University Press.

Henrichsen, Carsten: "*Retssikkerhed og moderne forvaltning – En retspolitisk studie i samspillet mellem stat, forvaltning og borger*", 1997, Akademisk Forlag.

Henricson, Ib: *"Politiret"*, 6. udgave, 2016, Jurist- og Økonomforbundets Forlag.

Henricson, Ib: *"International Politiret"*, 1. udgave, 2010, Jurist- og Økonomforbundets Forlag.

Hurwitz, Stephan: "*Den danske kriminalret Almindelig del, 4. reviderede udgave ved Knud Waaben"*, 1971, Gads Forlag.

Jakobsen, Søren Sandfeld (red.), Søren Johansen og Christian Bergqvist: *"Teleretten"*, 1. udgave, 2014, Jurist- og Økonomforbundets Forlag.

Jakobsen, Søren Sandfeld og Sten Schaumburg-Müller: "*Medieretten*", 1. udgave, 2013, Jurist- og Økonomforbundets Forlag.

Jensen, Sv. Gram: *"Almindelig retslære. En introduktion"*, 3. udgave, 1998, Jurist- og Økonomforbundets Forlag.

Jochimsen, Jørgen: *"Anonyme vidner og hemmelige agenter"*, 2003, Forlaget Thomson GadJura.

Jørgensen, Rikke Frank og Birgitte Kofod Olsen (red.): *"Privatliv i en Big Data tid"*, 2017, Gads Forlag.

Kistrup, Michael, Jakob Lund Poulsen, Jens Røn og Thomas Rørdam: *"Straffeprocessen"*, 3. udgave, 2018, Forlaget Thomson.

Kjølbro, Jon Fridrik: *"Den Europæiske Menneskerettighedskonvention for praktikere"*, 4. udgave, 2017, Jurist- og Økonomforbundets Forlag.

Lauridsen, Preben Stuer: "*Pressefrihed og personlighedsret*", 1988, Gyldendal.

Lauridsen, Preben Stuer: *"Retslæren"*, 1977, Akademisk Forlag.

Lorenzen, Peer, Sten Schaumburg-Müller, Jens Vedsted-Hansen, Peter Vedel Kessing, Jonas Christoffersen og Nina Holst Christensen: *"Den Europæiske menneskerettighedskonvention med kommentarer*", bind 1 og 2, 3. udgave, 2011, Jurist- og Økonomforbundets Forlag.

Moore, Sally Falk: *"Law as a Process*", New York, 1978, Routledge & Kegan Paul Ltd.

Munk-Hansen, Carsten: *"Retsvidenskabsteori"*, 2018, Jurist- og Økonomforbundets Forlag.

Nielsen, Gorm Toftegaard, Thomas Elholm og Morten Niels Jakobsen: *"Kommenteret straffelov – Speciel del"*, 11. udgave 2017, Jurist- og Økonomforbundets Forlag.

Nielsen, Gorm Toftegaard: *"Straffesagens gang"*, 6. udgave, 2016, Jurist- og Økonomforbundets Forlag.

Nielsen, Gorm Toftegaard: *"Strafferet 1- Ansvaret"*, 4. udgave, 2013, Jurist- og Økonomforbundets Forlag.

Nielsen, Jesper Løffler: *"IT-retlige metaproblemer med retsplejen som praktisk studie"*, 2017, Jurist- og Økonomforbundets Forlag.

Rainey, B., E. Wicks and C. Ovey, Jacobs, White and Ovey: "*The European Convention on Human Rights*", 7th edition, 2017, Oxford University Press.

Revsbech, Karsten , Jens Garde, Jørgen Albæk Jensen, Orla Friis Jensen, Helle Bødker Madsen og Søren Højgaard Mørup: "*Forvaltningsret. Almindelige emner*", 2016.

Ross, Alf og Jakob v. H. Holtermann: *"Om ret og retfærdighed: en indførelse i den analytiske retsfilosofi"*, Hans Reitzel, 2013.

Ross, Alf: "*Ret og retfærdighed En indførelse i den analytiske retsfilosofi*", 1966, Nyt Nordisk Forlag Arnold Busck.

Rytter, Jens Elo: *"Individets Grundlæggende Rettigheder"*, 3. udgave, 2019, Karnov Group.

Rønne, Anita, og Henrik Stevnsborg (red.): "*Ret SMART*", 2018, Jurist- og Økonomforbundets Forlag.
Satzger, Helmut: *"International and European Criminal Law"*, Second Edition, 2018, C. H. Beck, Hart and Nomos.

Schabas, William A.: "*The European Convention on Human Rights*", 2015, Oxford University Press.

Schaumburg-Müller, Sten: *"Fem retsfilosofiske teser"*, 2009, Jurist- og Økonomforbundets Forlag.

Sunde, Inger Marie: *"Datakriminalitet – en fremstilling af strafferettslige regler om datakriminalitet"*, 2016, Fagbokforlaget.

Sunde, Inger Marie: "*Automatisert inndragning*", 2010, Oslo.

Sunde, Inger Marie: *"Lov og rett i cyberspace"*, 2006, Fagbokforlaget.

Sørensen, Karsten Engsig og Jens Hartig Danielsen: *"EU-retten"*, 7. reviderede udgave, 2019, Jurist- og Økonomforbundets Forlag.

Trzaskowski, Jan (red.), Søren Sandfeld Jakobsen, Susanne Karstoft, Hanne Kirk, Lars Bo Langsted, Thomas Riis, Charlotte Bagger Tranberg & Helena Lybæk Guðmundsdóttir: *"Internetretten"*, 3. udgave 2017, Ex Tuto Publishing.

Tvarnø, Christina D. og Ruth Nielsen: *"Retskilder og retsteorier"*, 5. reviderede udgave, 2017, Jurist- og Økonomforbundets Forlag.

Udsen, Henrik: *"IT-ret"*, 3. udgave, 2016, samt 4. udgave 2019, Ex Tuto Publishing.

Vendius, Trine: *"Europol og cyberkriminalitet – Proaktiv efterforskning og forbrydelser mod børn"*, 1. udgave 2015, Ex Tuto Publishing.

Vestergaard, Jørn (red.), Dorph, Anders, Hanne Rahbæk, Jens Røn, og Thomas Rørdam: *"Forbrydelser - og andre strafbare forhold"*, 3. udgave, 2018, Forlaget Gjellerup.

Vestergaard, Jørn: *"Straffeproces – grundtræk af dansk strafferetspleje"*, 2. udgave, 2018, Forlaget Gjellerup.

Waaben, Knud: *"Strafferettens almindelige del. Ansvarslæren"*, 6. reviderede udgave ved Lars Bo Langsted, 2015, Karnov Group.

Waaben, Knud: *"Strafferettens specielle del"*, 6. reviderede udgave ved Lars Bo Langsted, 2014, Karnov Group.
Waaben, Knud: *"Strafferettens specielle del"*, 3. reviderede udgave, 1989, Gads Forlag.

Walden, Ian: *"Computer Crimes and Digital Investigations"*, 2.nd edition, 2016, Oxford University Press.

Artikler og antologi-bidrag:

Andersen, John Peter: "Provokationsgrænsen. Et par bemærkninger til det nye lovforslag om politiets anvendelse af agenter i efterforskningen", Juristen 1985, s. 179-185.

Andersen, Mads Bryde og Peter Landrock: "Kryptering og efterforskning", Juristen 1995, s. 306 ff.

Baumbach, Trine: "Hacker-bestemmelsen, Se og Hør-sagen og nyere tendenser", i "*I forskningens og formidlingens tjeneste – festskrift til professor Lars Bo Langsted"* (Sten Bønsing, Thomas Elholm, Søren Sandfeld Jakobsen og Lene Wacher Lentz, red.), 2018, Ex Tuto Publishing, s. 17-28.

Baumbach, Trine: "Den retsvidenskabelige strafferetsforskning i det 21. århundrede – refleksioner", TfK 2015.515.

Baumbach, Trine: "Om strafferetten i et menneskeretligt perspektiv, EU-ret og menneskeret", 2014.279.

Baumbach, Trine: "Det strafferetlige legalitetsprincip - i straffeloven og i Menneskerettighedskonventionen Om begrænset udvidende fortolkning og forudsigelighed", TfK 2013.105.

Baumbach, Trine: "Strafferetten og EU" i Trine Baumbach og Peter Blume (red.): *Retskildernes kamp – Forholdet mellem national offentlig ret og udefra kommende ret*", 2012, s. 49-70.

Baumbach, Trine: "Sportsvold – Er det strafbart? Om sport og strafferet", U 2009B.12.

Blume, Peter: "Databeskyttelse i den smarte verden" i "*Ret SMART – om smart teknologi og regulering"*, af Anita Rønne og Henrik Stevnsborg (red.), 2018, s. 40 ff.

Blume, Peter: "Privat censur", Juristen, nr. 1/2017.

Blume, Peter: ”Formålsbestemthed”, U 2016B.338.

Blume, Peter: ”Overvågning. Kan persondataretten gøre nytte?”, Nordisk Tidsskrift for Informationsvidenskab og Kulturformidling, årg. 3, nr. 2/3, 2014.

Blume, Peter og Janne Rothmar Herrmann: ”Se mig på nettet – om privatlivets ufred på sociale netværk og street view”, Juristen, nr. 4/2010.

Bønsing, Sten: ”Embedsmænds pligter -en kommentar til ”Kodex VII – Syv centrale pligter for embedsmænd i centraladministrationen”, U 2016.B.33.

Chedraui, Ana María Torres: ”An analysis of the exclusion of evidence obtained in violation of human rights in light of the jurisprudence of the European Court of Human Rights”, Tilburg Law Review 2010, volume 15, issue 2.

Dahl, Børge: ”Dynamiske domstole, retssikkerhed og demokrati: Skal menneskerettigheder udvikles af politikere eller dommere?” Juristen nr. 5/2017.

Dalberg-Larsen, Jørgen: ”Nogle bemærkninger om begrebet retlig pluralisme”, i ”*Ikke kun retsfilosofi – Festskrift til Sten Schaumburg –Müller*”, af Nis Jul Clausen, Jørgen Dalberg-Larsen, Bent Ole Gram Mortensen og Hans Viggo Godsk Pedersen (red.) 2016, Jurist- og Økonomforbundets Forlag.

Dalberg-Larsen, Jørgen: ”The Unity of Law: An Illusion? On Legal pluralism in Theory and Practice”, Mobility and Norm Change, Volume 2, 2000.

Dalberg-Larsen, Jørgen: ”Hvad er retssikkerhed, og hvordan kan den fremmes”, i ”*Liv, arbejde og forvaltning*”, af Peter Blume, Kirsten Ketscher og Steen Rønsholdt (red.), GadJura, 1995, s. 121 ff.

Dalgas Rasmussen, Ib: ”Om grænser for politiets agenter”, Juristen 1985, s. 280.

Edwards, Lilian and Lachlan Urquhart:”Privacy in Public Spaces: What Expectations of Privacy Do We Have in Social Media Intelligence?” (December 11, 2015). International Journal of Law and Information Technology (Autumn 2016) 24 (3), 279-310 . Available at SSRN: https://ssrn.com/abstract=2702426 or http://dx.doi.org/10.2139/ssrn.2702426

Elholm, Thomas: ”Det retlige forbehold og strafferetten” i ”*EU-retten i Danmark*” af Birgitte Egelund Olsen og Karsten Engsig Sørensen (red.), 2018, Jurist- og Økonomforbundets Forlag, s. 87-104.

Elholm, Thomas: ”Sanktionering af EU-retten” i ”*EU-retten i Danmark*” (Birgitte Egelund Olsen og Karsten Engsig Sørensen, red.), 2018, Jurist- og Økonomforbundets Forlag, s. 265-288.

Freitas, Pedro Miguel F. & Nuno Gonçalves (2015): ”Illegal access to information systems and the Directive 2013/40/EU”, International Review of Law, Computers and Technology, 29:1, s. 50-62.

Gammeltoft Hansen, Hans: ”Om definitionen af straffeprocessuelle tvangsindgreb” i *”Jurist uden omsvøb - Festskrift til Gorm Toftegaard Nielsen”,* Annette Møller-Sørensen og Anette Storgaard (red.), 2007, Christian Ejlers’ Forlag, s. 139-148.
Gammeltoft-Hansen, Hans: ”Agent Controlleur”, Tidsskrift for Rettsvitenskap nr. 1-2, 1984.

Gammeltoft-Hansen, Hans: ”Om afgrænsningen af ”straffeprocessuelle tvangsindgreb””, U 1979B.1.

Gomard, Bernhard: ”Analogi i strafferetten” i ”*Festskrift til Alf Ross*” af Mogens Blegvad, Max Sørensen, Isi Foighel, Jørgen Trolle og A. Vinding Kruse (red.), 1969, Juristforbundets Forlag, s. 125-152.

Gomard, Bernhard: ”Den tekniske udvikling og retssystemet”, U 1963B.205.

Greve, Vagn: ”Om hjemmelen for administrative straffebestemmelser”, i ”*Lov og Frihet Festskrift til Johs. Andenæs*” af Anders Bratholm, Nils Christie og Torkel Opsahl (red.), 1982, Oslo Universitetsforlag.

Griffiths, John: "What is Legal Pluralism" in *Journal of Legal Pluralism,* (1986) 24: 1-55.

Henrichsen, Carsten: ”Retssikkerhed – en begrebsanalyse”, i ”*Retlig polycentri*” af Peter Blume og Hanne Petersen (red.), 1993, s. 309 f.

Horder, Jeremy: *”Ashworths’s Principles of Criminal Law*”, 9th Edition, 2019.

Høyer, Thorkild: ”Politiagenter og narkotika”, U 1988B.178.

Jakobsen, Søren Sandfeld: ”Misinformation (”fake news”) i retlig belysning”, Juristen 1/2019.

Kallehauge, H: ”Replik vedrørende utraditionel efterforskning - agents provocateurs”, U 1979B.28.

Kallehauge, H: ”Utraditionel efterforskning – agentes provocateurs”, U 1978B.85.

Kallehauge, H: ”Agent Provocateur – En efterforskningsmetode”, U 1976B.1.

Kaltenborn, Jul Fredrik: *”Teknologinøytralitet og datakriminalitet – særlig om klassifiseringen av begrebet datasystem”*, Tidsskrift for Strafferett, nr. 2-2019, s. 148-167.

Kerr, Orin S.: ”Norms of computer trespass (essay)”, *Colombia Law Review*, 1143 (2016).

Kerr, Orin S.: ”Vagueness Challenges to the Computer Fraud and Abuse Act” (*Symposium: Cyberspace & the Law: Privacy, Property and Crime in the Virtual Frontier)* 94 Minnesota Law Review, s. 1561, 2010.

Kjølbro, Jon Fridrik: ”Den Europæiske Menneskerettighedsdomstol: Praktiske udfordringer, juridiske udfordringer og et spørgsmål om legitimitet”, Juristen nr. 5/2017.

Koch, Pernille Boye: ”Lovgivers rolle som fortolker af internationale retskilder – på hvilken måde gælder menneskerettighederne i Danmark”, Tidsskrift for Rettsvitenskap, nr. 1/2019.

Koops, Bert Jaap: ”Should ICT Regulation Be Technology-Neutral?” in ” Starting Points for ICT Regulation. Deconstructing Prevalent Policy One-Liners”, IT & LAW SERIES, Bert-Jaap Koops, Miriam Lips, Corien Prins & Maurice Schellekens, eds., Vol. 9, pp. 77-108, The Hague: T.M.C. Asser Press, 2006. Available at SSRN: https://ssrn.com/abstract=918746

Langsted, Lars Bo: ”Efterforskning på udenlandske servere”, Juristen nr. 3/2018, s. 94-98.

Langsted, Lars Bo: ”Commentary: commentary to Supreme Court Order U 2012.2614 H”, Digital Evidence and Electronic Signature Law Review, 10 (2013), s. 164-165.

Larsen, Torsten Bjørn og Rasmus Kristian Felthusen: ”De sociale mediers brugervilkår del I – Aftalen”, *Erhvervsjuridisk Tidsskrift*, 2016.266.

Lentz, Lene Wacher: ”Efterforskningens grænser på internettet”, s. 137-151, i ”*Eksponeret – Grænser for privatliv i en digital tid*”, red.: Rikke Frank Jørgensen og Birgitte Kofod Olsen, 2018, Gadjura.

Lentz, Lene Wacher: ”Hemmelig ransagning og brevstandsning i den digitale virkelighed”, Juristen nr. 1, 2016.

Madsen, Lasse Lund: ”Edition som efterforskningsmiddel – med særligt henblik på internetrelaterede bedragerisager”, U 2017B. 205.

Madsen, Lasse Lund: ”Agentvirksomhed online – efterforskning i IT-relaterede sager om misbrug af børn”, U 2017B.95.

Madsen, Lasse Lund: ”Er vold altid strafbar? – om vold mellem idrætsudøvere”, U 2009B.183.

Manniche, Steen: ”Er data neutralt?” i ”*Ret SMART – om smart teknologi og regulering”*, af Anita Rønne og Henrik Stevnsborg (red.), 2018, s. 35 f.

Marry, Sally Engle: ”Legal Pluralism”Law & Society Review, Vol. 22, No. 5 (1988), pp. 869-896.

Mathiesen, Peter Dueholm: ”Virtuelle ting – Kan virtuelle ting strafferetligt karakteriseres eller ligestilles som rørlige ting?” Nordisk Tidsskrift for Kriminalvidenskab, 2014, s. 51.

Mathiesen, Peter Dueholm: ”Cloud computing og den strafferetlige beskyttelse af data”, TfK 2013.240.

Moise, Adrian Christian (2015): ”Analysis of Directive 2013/40/EU on attacks against information systems in the context of approximation of law at the European level”, Journal of Law and Administrative Sciences, Special Issue, s. 374-383.
Munk-Hansen, Carsten: ”Retssikkerhedshensynet”, Kapitel 1 i ”Retssikkerhed i konkurrence med andre hensyn” af Carsten Munk-Hansen og Trine Schultz (red.), 2012, Jurist- og Økonomforbundets Forlag, s. 15-32.

Murphy, Cian C.: ”The Principle of Legality in Criminal Law under ECHR”, (November 16, 2009) i European Human Rights Law Review, Vol. 2, 2010.

Nielsen, Gorm Toftegaard: ”Hvad er et tvangsindgreb? Om straffeproces og forvaltningsret”, Juristen 2005, nr. 5, s. 153.

Nissen, Volmer: ”Om meddelere, agenter, politifolk og vidner”, U 1988B.117.
Pedersen, Anja Møller, Henrik Udsen og Søren Sandfeld Jakobsen: ”Data retention in Europe – the Tele 2 case and beyond”, International Data Privacy Law, 2018, Vol. 8, No. 2.

Petersen, Hanne: ”Globalisering og retspluralisme – Juridiske begreber i forandring” i ”*Retlig mangfoldighed – En fælles udfordring for retsvidenskab og antropologi*” af Sten Schaumburg-Müller & Bodil Selmer (red.):, 2003, s. 15 ff.

Rasmussen, Elsebeth: ”Hvem er agent?”, U 1987B.396.

Reimer, Stefan: ”Polisens arbetsmetoder och straffprocessuella rättsäkerhetsprinciper” i *”Festskrift til Per Ole Träskman”* af Ulrika Andersson, Christoffer Wong og Helén Örnemark Hansen (red.), 2011, Norstedts Juridik.

Rønsholdt, Steen: ”Om retssikkerhed og andre hensyn, i ”*Retlig polycentri*” af Peter Blume og Hanne Petersen (red.), 1993, s. 340.

Schaumburg-Müller, Sten: ”Det hypotetiske samtykke” i ”*Festskrift til Hans Viggo Godsk Pedersen*” af Nis Jul Clausen, Annette Kronborg, Nina Dietz Legind og Bent Ole Gram Mortensen (red.), 2017, Jurist- og Økonomforbundets Forlag.

Schaumburg-Müller, Sten: ”Borgerlig privathed i en digitaliseret verden”, Nordisk Juridisk Tidsskrift Retfærd, nr. 1, 2016, s.45 ff.

Schaumburg-Müller, Sten: ”Kritik af den rene retspluralisme” begge i ”*Retlig mangfoldighed – En fælles udfordring for retsvidenskab og antropologi*” af Sten Schaumburg-Müller & Bodil Selmer (red.):, 2003.

Slumstrup, Jacob: ”Indhentelse af teleoplysninger med tilbagevirkende kraft”, U 1993B.399.

Smith, Eva: ”Højesteret og Den Europæiske Menneskerettighedskonvention”, Juristen nr. 2/2018.

Štarienė, Lijana: ”The limits of the use of undercover agents and the right to a fair trial under Article 6(1) of the European Convention on Human Rights”, University of Wroclaw, Jurisprudence, 2009, 3(117), p. 263-284.

Sunde, Inger Marie: ”Har vi behov for straffebud om datakriminalitet?” i ”*I forskningens og formidlingens tjeneste – festskrift til professor Lars Bo Langsted*” af Sten Bønsing, Thomas Elholm, Søren Sandfeld Jakobsen og Lene Wacher Lentz (red.), 2018, Ex Tuto Publishing, s. 309-325.

Sunde, Inger Marie: ”Cybercrime Law”, i *”Digital Forensics”* af André Årnes (ed.), 2018, Wiley, s. 51-115.

Sunde, Inger Marie: ”Dataavlesing” i Tidsskriftet Retfærd 35, 2012, nr. 1/136.
Teubner, Gunther: ”Global Bukowina: Legal Pluralism in the World-Society” i *”Global Law Without a State”* af Gunther Teubner (ed.), Dartsmouth, pp. 3-28, 1996. Available at SSRN: https://ssrn.com/abstract=896478

Udsen, Henrik: ”Digitale freds- og ærekrænkelser – mellem strafferet og persondataret” i ”*Festskrift til Mads Bryde Andersen*” af Henrik Udsen, Jan Schans Christensen, Jesper Lau Hansen, Torsten Iversen og Linda Nielsen (red.), 2018, Jurist- og Økonomforbundets Forlag, s. 121-146.

Udsen, Henrik: ”Behandling af offentliggjorte personoplysninger – særligt om sociale netværkstjenester” i ”*Ret, informatik og samfund – festskrift til Peter Blume*”, Carsten Henrichsen, Jens Elo Rytter og Steen Rønsholdt (red.), 2010, s. 321.
Vedsted-Hansen, Jens: ”Danske udfordringer i det europæiske menneskerettighedssystem”, Juristen nr. 6/2017.

Vestergaard, Jørn: ”EU-strafferetten og individets grundlæggende rettigheder”, TfK 2016.429.

Vestergaard, Jørn: ”Den europæiske arrestordre – udlevering til strafforfølgning mv.”, TfK 2004.555.

Volquartzen, Mette: ”Forskydninger mellem det private og det offentlige i smart politiarbejde”, s. 171-189 i ”*Ret SMART*”, Anita Rønne og Henrik Stevnsborg (red.), 2018.

Waaben, Knud: ”Lovkravet i strafferetten”, Nordisk Tidsskrift for Kriminalvidenskab, 1994.